VirusScan para Windows 3.1*x*

Guia do Usuário

Network Associates Brazil
Rue Geraldo Flauzino Gomes 78-cj.51
04575-060 Sao Paulo
Brasil
Tél. : 55 11 550 51009
Fax : 55 11 550 51006

CONTRATO DE LICENÇA:

NOTA PARA TODOS OS USUÁRIOS: LEIA COM ATENÇÃO O SEGUINTE CONTRATO LEGAL ("CONTRATO"), QUE ESTABELECE OS TERMOS GERAIS DA LICENÇA PARA O SOFTWARE DA NETWORK ASSOCIATES. PARA OBTER OS TERMOS ESPECÍFICOS DA SUA LICENÇA, CONSULTE OS ARQUIVOS README.1ST E LICENSE.TXT, OU OUTRO DOCUMENTO DE LICENÇA QUE ACOMPANHE O SEU SOFTWARE, EM FORMA DE ARQUIVO DE TEXTO OU COMO PARTE DA EMBALAGEM DO SOFTWARE. SE VOCÊ NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS ANTERIORMENTE, NÃO INSTALE O SOFTWARE. (SE FOR APLICÁVEL, VOCÊ PODE DEVOLVER O PRODUTO AO LOCAL DE AQUISIÇÃO PARA OBTER UM REEMBOLSO TOTAL.)

1. **Concessão de Licença.** Sujeito a pagamento dos honorários de licença aplicáveis e à aceitação dos termos e condições deste Contrato, a Network Associates lhe concede pelo presente documento o direito não exclusivo e não transferível de usar uma cópia da versão especificada do Software e da documentação que o acompanha (a "Documentação"). Você pode instalar uma cópia do Software em seu computador, estação de trabalho, assistente digital pessoal, pager, "telefone inteligente" ou outro dispositivo eletrônico para o qual se destina o Software (cada um deles, um "Dispositivo Cliente"). Se o Software for licenciado como um conjunto ou fizer parte de um pacote com mais de um produto de Software especificado, esta licença aplica-se a todos os produtos de Software especificados, que estão sujeitos a quaisquer restrições ou períodos de uso especificados individualmente para cada um desses produtos de Software na embalagem ou fatura do produto aplicável.

   a. **Utilização.** O Software é licenciado como um produto único; não pode ser usado em mais de um Dispositivo Cliente ou por mais de um usuário de cada vez, exceto como estabelecido na Seção 1. O Software está "em uso" num computador quando estiver carregado na memória temporária (isto é, memória de acesso aleatório ou RAM) ou instalado na memória permanente (por exemplo, disco rígido, CD-ROM ou outro dispositivo de armazenamento) desse Dispositivo Cliente. Esta licença o autoriza a fazer uma cópia do Software somente para backup ou para arquivamento, contanto que essa cópia contenha todas as informações relativas à propriedade do software.

   b. **Utilização do Modo de Servidor.** De acordo com o estabelecido na embalagem ou fatura do produto aplicável, você pode instalar e usar o Software em um Dispositivo Cliente ou em um servidor ("Servidor") em um ambiente de rede ou multiusuário ("Utilização do Modo de Servidor") para (i) conectar-se, direta ou indiretamente, com um número que não exceda o máximo de Dispositivos Clientes ou "estações" especificados; ou (ii) distribuir não mais do que o número máximo de agentes (pollers) especificados para distribuição. Se a embalagem ou fatura do produto aplicável não

especificar o número máximo de Dispositivos Clientes ou pollers, esta licença lhe concede uma licença para usar um único produto, sujeita às cláusulas da sub-seção (a), acima. É necessária uma licença individual para cada Dispositivo Cliente ou estação que possa ser conectado ao Software em qualquer momento, mesmo que esses Dispositivos Clientes ou estações não estejam conectados ao Software de forma concorrente, ou estejam usando o Software em qualquer momento determinado.

A utilização de software ou hardware que reduza o número de Dispositivos Clientes ou estações conectadas que usem o Software simultaneamente (por exemplo, o uso de software ou hardware de "multiplexação" ou "pesquisa seqüencial") não reduz o número total de licenças que você deve obter. Especificamente, o número de licenças deve ser igual ao número de entradas distintas para o "front end" do software ou hardware de multiplexação ou pesquisa seqüencial. Se o número de Dispositivos Clientes ou estações que podem ser conectados ao Software exceder o número de licenças obtidas, você deve ter um mecanismo razoável que assegure que a utilização do Software não ultrapasse os limites especificados na fatura ou na embalagem do produto. Esta licença o autoriza a fazer uma cópia ou efetuar o download da Documentação para cada Dispositivo Cliente ou estação licenciada, desde que cada cópia contenha todas as informções de propriedade da Documentação.

c. **Utilização Múltipla.** Se o Software estiver licenciado para uso múltiplo, de acordo com o especificado na embalagem ou fatura do produto, você poderá fazer, usar e instalar em Dispositivos Clientes quantas cópias adicionais do Software quiser, de acordo com as especificadas nos termos de licença de uso múltiplo. Esta licença o autoriza a fazer uma cópia da Documentação, ou obtê-la por download, para cada cópia do Software de acordo com os termos do uso múltiplo, desde que cada cópia contenha todas as informações de propriedade da Documentação. Você deve ter um mecanismo razoável de controle para assegurar que o número de Dispositivos Clientes nos quais o Software está instalado não ultrapasse o número de licenças adquiridas.

2. **Duração.** Esta licença vigora pelo período especificado na fatura ou embalagem do produto, ou nos arquivos README.1ST, LICENSE.TXT, ou outro arquivo de texto que acompanhe o Software e que tenha o objetivo de estabelecer a duração do seu contrato de licença.. As instâncias que no Contrato estabelecido neste documento entrarem em conflito com as cláusulas da embalagem ou fatura do produto, os documentos README.1ST e LICENSE.TXT, a fatura do produto, a embalagem ou outro documento de texto se constituirão nos termos da sua concessão de licença para uso do Software. Você ou a Network Associates podem terminar a sua licença antes do período especificado no documento adequado de acordo com os termos estabelecidos anteriormente. Este Contrato e a sua licença cessarão automaticamente se você não cumprir com qualquer uma das limitações ou outros requisitos descritos. Ao final deste contrato, você deve destruir todas as cópias do Software e da Documentação. Este contrato pode ser rescindido a qualquer momento, destruindo-se todas as cópias do Software e a Documentação, bem como todas as cópias do Software e da Documentação.

3. **Atualizações.** Durante o período em que vigore a sua licença, você pode fazer download de revisões, atualizações de versão ou de atualizações do Software quando a Network Associates as publicar no seu sistema de quadro de avisos eletrônico, site da web ou através de outros serviços online.

4. **Direitos de Propriedade.** O Software e a Documentação são protegidos pelas leis de direito autoral dos Estados Unidos e pelas cláusulas dos tratados internacionais. A Network Associates possui e detém todos os direitos, titularidade e participações em relação ao Software, incluindo todos os direitos autorais, patentes, direitos sobre segredos comerciais, marcas comerciais e outros diretos de propriedade estabelecidos anteriormente. Você reconhece que a posse, instalação ou uso do Software não lhe transfere qualquer direito à propriedade intelectual do Software e que não adquirirá quaisquer direitos sobre o Software exceto os expressamente estabelecidos neste Contrato. Você concorda que quaisquer cópias do Software e da Documentação.

5. **Restrições.** Não é permitido alugar, arrendar, emprestar ou revender o Software, ou permitir que terceiros se beneficiem do uso e dos recursos do Software através de compartilhamento de tempo, birô de serviços ou qualquer outro tipo de acordo. Não é permitido transferir qualquer direitos que lhe foi concedido por este Contrato. Não é permitido copiar a documentação que acompanha o Software. Não é permitido utilizar engenharia reversa, descompilar ou desassemblar o Software, exceto se esta restrição for expressamente proibida pelas leis vigentes. Não é permitido modificar ou criar trabalhos derivados com base no Software, no todo ou em parte. Não é permitido copiar o Software, exceto o expressamente permitido na Seção 1 acima. Não é permitido remover quaisquer informações relativas à propriedade ou rótulos do Software. Todos os diretos não expressamente aqui estabelecidos são reservados à Network Associates. A Network Associates se reserva o direito de conduzir auditorias periódicas, antecedidas por comunicação escrita, para verificar o cumprimento dos termos deste Contrato.

6. **Garantia e Renúncia à Garantia**

   a. **Garantia Limitada.** A Network Associates garante que por um período de trinta (30) dias a partir da data da compra original da mídia (por exemplo, os disquetes) no qual o Software está contido, esta não apresentará defeitos de fabricação.

   b. **Indenização do Cliente.** A responsabilidade da Network Associates e de seus fornecedores será, a critério da Network Associates, (i) devolver o valor pago pela licença, se houver, ou (ii) substituir a mídia defeituosa na qual o Software estiver contido por uma cópia da mídia livre de defeitos. Você deve devolver a mídia defeituosa à Network Associates por sua conta, com uma cópia de seu recibo. Esta garantia limitada é anulada se o defeito tiver sido provocado por um acidente, uso indevido ou má utilização. Qualquer mídia de substituição será garantida pelo período restante da garantia original. Fora dos Estados Unidos da América, essa indenização não está disponível na medida em que a Network Associates está sujeita às restrições das leis e normas que regulam a exportação dos Estados Unidos.

Renúncia à Garantia. Renúncia à Garantia. Dentro dos limites da legislação em vigor e da garantia limitada aqui estabelecida, O SOFTWARE É FORNECIDO SEM GARANTIAS DE QUALQUER NATUREZA, EXPRESSAS OU IMPLÍCITAS, DA FORMA EM QUE SE ENCONTRA. SEM LIMITAR AS CLÁUSULAS ANTERIORES, VOCÊ ASSUME A RESPONSABILIDADE DA ESCOLHA DO SOFTWARE PARA ATINGIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, USO E RESULTADOS OBTIDOS COM ESTE SOFTWARE. SEM LIMITAR AS CLÁUSULAS ANTERIORES, A NETWORK ASSOCIATES NÃO GARANTE QUE O SOFTWARE ESTEJA LIVRE DE ERROS, INTERRUPÇÕES OU OUTROS TIPOS DE FALHAS, OU QUE O SOFTWARE ATENDERÁ ÀS SUAS NECESSIDADES. DENTRO DOS LIMITES DA LEGISLAÇÃO EM VIGOR, A NETWORK ASSOCIATES NEGA TODAS AS GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO MAS NÃO LIMITANDO-SE A GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM DETERMINADO OBJETIVO E À NÃO VIOLAÇÃO DE DIREITOS EM RELAÇÃO AO SOFTWARE E À DOCUMENTAÇÃO QUE O ACOMPANHA. ALGUNS PAÍSES E JURISDIÇÕES NÃO PERMITEM LIMITAÇÕES EM GARANTIAS IMPLÍCITAS, POR ISSO AS LIMITAÇÕES ACIMA PODEM NÃO SE APLICAR A VOCÊ. As cláusulas anteriores serão aplicadas dentro dos limites máximos permitidos pela legislação em vigor.

A compra ou pagamento do Software pode lhe dar direito a garantia adicionais, que a Network Associates especificará na embalagem ou fatura que você irá receber ao adquirir o produto ou no README.1ST , LICENSE.TXT ou outro arquivo de texto que acompanhe o Software e estabeleça os termos de seu contrato de licença. Nos casos em que as cláusulas deste Contrato entrem em conflito com as cláusulas da embalagem ou fatura do produto, o README.1ST, LICENSE.TXT ou documentos semelhantes, a fatura, embalagem ou arquivo de texto estabelecerá os termos de seus direitos de garantia para o Software.

7. **Limitação de Responsabilidade.** EM NENHUMA CIRCUNSTÂNCIA, SEM QUALQUER PRETEXTO LEGAL, SEJA ATO ILÍCITO, CONTRATO OU QUALQUER OUTRA CIRCUNSTÂNCIA, A NETWORK ASSOCIATES OU SEUS FORNECEDORES PODEM SE RESPONSABILIZAR POR VOCÊ OU POR QUALQUER OUTRA PESSOA EM CONSEQÜÊNCIA DE QUALQUER DANO INDIRETO, INCIDENTAL OU CONSEQÜENTE DE QUALQUER NATUREZA INCLUINDO, SEM LIMITAÇÃO, PREJUÍZOS POR PERDAS E DANOS, INTERRUPÇÃO DO TRABALHO, FALHA OU MAU FUNCIONAMENTO DO COMPUTADOR, OU QUAISQUER OUTROS DANOS OU PERDAS. EM NENHUM CASO A NETWORK ASSOCIATES SERÁ RESPONSABILIZADA POR QUAISQUER DANOS ACIMA DO PREÇO DE VENDA QUE A NETWORK ASSOCIATES COBRA POR UMA LICENÇA DO SOFTWARE, MESMO QUE A NETWORK ASSOCIATES TENHA SIDO AVISADA SOBRE A POSSIBILIDADE DE TAIS DANOS. O LIMITE DE RESPONSABILIDADE NÃO DEVE SER APLICADO À RESPONSABILIDADE POR MORTE OU FERIMENTOS PESSOAIS DENTRO DOS LIMITES LEGAIS EM VIGOR QUE PROÍBEM TAIS LIMITAÇÕES. ALÉM DISSO, ALGUNS ESTADOS E JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO OU LIMITAÇÃO DE DANOS INCIDENTAIS OU CONSEQÜENTES, POR ISSO TAL

LIMITAÇÃO E EXCLUSÃO PODE NÃO SE APLICAR A VOCÊ. As cláusulas anteriores serão aplicadas dentro dos limites máximos permitidos pela legislação em vigor.

8. **Governo dos Estados Unidos.** O Software e a Documentação que o acompanha são considerados "software comercial de computador" e "documentação comercial de software de computador", respectivamente, de acordo com a Seção 227.7202 do DFAR e a Seção 12.212 do FAR conforme aplicável. Qualquer uso, modificação, reprodução, versão, execução, exibição ou divulgação do Software e da Documentação, que o acompanha, pelo Governo dos Estados Unidos serão governadas somente pelos termos deste Contrato e proibidas exceto no âmbito expressamente permitido pelos termos deste Contrato.

9. **Controles de Exportação.** É proibido exportar, reexportar ou fazer download do Software, da Documentação, das informações ou tecnologia neles contidas de nenhum modo (i) para (ou para um cidadão ou residente de) Cuba, Irã, Iraque, Líbia, Coréia do Norte, Sudão, Síria ou qualquer país para o qual os Estados Unidos da América tenham estabelecido embargo de produtos; ou (ii) para qualquer pessoa que conste na lista de Nações Especialmente Designadas (Specially Designated Nations) do Departamento do Tesouro Americano ou na Tabela de Pedidos Negados (Table of Denial Orders) do Departamento de Comércio Americano. Ao fazer download ou usar o Software, você estará aceitando as cláusulas anteriores e certificando que não está localizado em, sob o controle de, ou é cidadão ou residente em nenhum desses países, ou não consta das listas supra citadas.

   ALÉM DISSO, VOCÊ DEVE ESTAR CIENTE DE QUE A EXPORTAÇÃO DO SOFTWARE É RESTRITA A EXPORTAÇÃO E REEXPORTAÇÃO DE CERTOS PRODUTOS E DADOS TÉCNICOS. SE A EXPORTAÇÃO DO SOFTWARE FOR CONTROLADA POR ESTAS REGRAS E NORMAS, ENTÃO O SOFTWARE NÃO DEVE SER EXPORTADO OU REEXPORTADO, DIRETA OU INDIRETAMENTE, (A) SEM TODAS AS LICENÇAS PARA EXPORTAÇÃO OU REEXPORTAÇÃO E AS APROVAÇÕES GOVERNAMENTAIS DOS ESTADOS UNIDOS DA AMÉRICA OU OUTRAS PERTINENTES DITADAS POR QUAISQUER LEIS APLICÁVEIS, OU (B) VIOLANDO QUALQUER PROIBIÇÃO APLICÁVEL À EXPORTAÇÃO OU REEXPORTAÇÃO DE QUALQUER PARTE DO SOFTWARE. ALGUNS PAÍSES FAZEM RESTRIÇÕES AO USO DE CRIPTOGRAFIA DENTRO DE SUAS FRONTEIRAS, OU À IMPORTAÇÃO OU EXPORTAÇÃO DE CRIPTOGRAFIA MESMO QUE SOMENTE PARA USO COMERCIAL OU PESSOAL TEMPORÁRIO. VOCÊ ESTÁ DE ACORDO QUE A IMPLEMENTAÇÃO E O CUMPRIMENTO DESSAS LEIS NEM SEMPRE É CONSISTENTE EM RELAÇÃO A PAÍSES ESPECÍFICOS. EMBORA OS SEGUINTES PAÍSES NÃO CONSTITUAM UMA LISTA EXAUSTIVA, PODEM EXISTIR RESTRIÇÕES À EXPORTAÇÃO DE TECNOLOGIA CRIPTOGRAFADA PARA, OU IMPORTAÇÃO DA: BÉLGICA, CHINA (INCLUINDO HONG KONG), FRANÇA, ÍNDIA, INDONÉSIA, ISRAEL, RÚSSIA, ARÁBIA SAUDITA, CINGAPURA E CORÉIA DO SUL. VOCÊ CONFIRMA QUE É DE SUA RESPONSABILIDADE CUMPRIR AS LEIS DE EXPORTAÇÃO DO GOVERNO E OUTRAS LEIS APLICÁVEIS, E QUE A NETWORK ASSOCIATES NÃO TEM MAIS NENHUMA RESPONSABILIDADE APÓS A VENDA INICIAL PARA VOCÊ NO TERRITÓRIO DE ORIGEM DA VENDA.

10. **Atividades de Alto Risco.** O Software não é tolerante a falhas e não foi projetado nem destina-se ao uso em ambientes perigosos que necessitem de dispositivos de proteção contra falhas, incluindo mas não se limitando, durante a operação de plantas nucleares, navegação aérea ou sistemas de comunicação, controle de tráfego aéreo, sistemas de armamentos, máquinas de suporte direto à vida, ou qualquer outra aplicação na qual uma falha do software possa causar a morte, danos pessoais ou danos severos físicos ou de propriedade (coletivamente chamadas de "Atividades de Alto Risco"). A Network Associates renuncia expressamente a qualquer garantia, expressa ou implícita de adequação a Atividades de Alto Risco.

11. **Diversos.** Esse Contrato é governado pelas leis dos Estados Unidos e do Estado da Califórnia, sem fazer referência a conflitos de princípios legais. A aplicação da United Nations Convention of Contracts for the International Sale of Goods está expressamente excluída. O Contrato estabelecido neste documento tem caráter de recomendação e não substitui as cláusulas de qualquer Contrato estabelecido nos arquivos README.1ST e LICENSE.TXT, ou qualquer outro arquivo de texto que acompanhe o Software e pretenda estabelecer os termos do seu contrato de licença. Nos casos em que as cláusulas deste Contrato entrem em conflito com as cláusulas do documento README.1ST ou LICENSE.TXT, o documento de texto se constituirá nos termos da sua concessão de licença para uso do Software. Este Contrato não pode ser modificado, exceto através de um adendo por escrito, emitido por um representante da Network Associates devidamente autorizado. Nenhuma cláusula a este respeito pode ser desconsiderada a menos que essa desistência de direito seja feita por escrito e assinada pela Network Associates ou pelo seu representante devidamente credenciado. Se qualquer cláusula deste Contrato for invalidada, o restante deste Contrato continuará em vigor. As partes confirmam que é de seu desejo que este Contrato seja redigido somente em Português.

12. **Contato para o Cliente da Network Associates.** Se você tiver perguntas a fazer sobre esses termos e condições, ou se quiser entrar em contato com a Network Associates por outra razão, ligue para (408) 988-3832, fax (408) 970-9727, escreva para a Network Associates, Inc. no endereço 3965 Freedom Circle, Santa Clara, California 95054, EUA, ou visite o site da Web da Network Associates em http://www.nai.com.

Prefácio

O que aconteceu?

Se você já perdeu arquivos importantes armazenados no seu disco rígido, vendo-os desaparecer enquanto o seu computador pára a fim de exibir uma saudação juvenil de uma pessoa maliciosa no seu monitor, ou se passou pela situação de ter que se desculpar por causa de mensagens de correio eletrônico insultantes nunca enviadas, saberá em primeira mão como os vírus de computador e outros programas destrutivos podem interromper a sua produtividade. Se o seu computador ainda não tiver sido infectado por vírus, você pode colocar-se entre os que têm sorte. Porém, com mais de 16.000 vírus conhecidos em circulação, capazes de atacar sistemas de computador com base em Windows e DOS, trata-se apenas de uma questão de tempo para que isto aconteça com você.

A boa notícia é que, dos milhares de vírus circulantes, apenas um pequeno número, comparativamente, causa reais danos aos seus dados. De fato, o termo “vírus de computador” identifica uma ampla lista de programas que têm somente um recurso em comum: “reproduzirem-se” automaticamente ao anexarem-se ao software host ou aos setores de disco de seu computador, normalmente, sem o seu conhecimento. A maioria dos vírus causa problemas relativamente triviais, que variam dos que apenas perturbam aos completamente insignificantes. Freqüentemente, a principal conseqüência de uma infecção por vírus é o tempo e o esforço gastos para descobrir a origem da infecção e erradicar todos os seus traços.

Por que se preocupar?

Por que a preocupação com as infecções por vírus, se a maioria dos ataques causam poucos danos? O problema tem duas partes: primeira, embora relativamente poucos vírus tenham efeito danoso, isso não explica a extensão da infecção pelos vírus destrutivos. Em muitos casos, os vírus com os efeitos altamente prejudiciais são os mais difíceis de serem detectados — o programador de vírus que se dedica a causar danos tomará medidas extras para evitar a detecção. Segunda, mesmo os vírus relativamente “benignos” podem interferir na operação normal de seu computador e causar comportamentos imprevisíveis em outros softwares. Alguns vírus contêm bugs, código escrito precariamente, ou outros problemas bastante sérios que causam pane quando são executados. Outras vezes, softwares legítimos têm

problema de execução quando um vírus tiver, intencionalmente ou não, alterado os parâmetros do sistema ou outros aspectos do ambiente de computação. Buscar a origem das panes ou congelamentos de sistema resultantes gasta tempo e dinheiro que poderiam ser empregados em atividades mais produtivas.

Acima desses problemas está o da percepção: uma vez infectado, o seu computador pode servir como uma origem de infecção para outros computadores. Se você trocar dados com seus colegas ou clientes freqüentemente, poderá passar à frente um vírus, sem saber, que poderia causar mais danos à sua reputação ou aos seus contatos com outras pessoas do que ao seu computador.

A ameaça dos vírus e outros softwares destrutivos é real e piora cada vez mais. A International Computer Security Association estimou em US$ 1 bilhão por ano o custo total, no mundo inteiro, com perda de tempo e produtividade simplesmente para detectar e limpar infecções por vírus, um número que não engloba os custos com a perda e recuperação de dados durante os ataques que os destruíram.

Qual a origem dos vírus?

Quando você ou um de seus colegas recupera o sistema de um ataque de vírus ou ouve falar de novas formas de softwares destrutivos que aparecem em programas usados comumente, deve se perguntar como nós, usuários de computadores, chegamos a esse ponto. Qual a origem dos vírus e de programas destrutivos? Quem os escreve? Por que aqueles que os criam procuram interromper o fluxo de trabalho, destruir dados ou fazer com que pessoas percam tempo e dinheiro para erradicá-los? O que pode fazê-los parar?

Por que isso aconteceu comigo?

Não deve ser um grande consolo ouvir que o programador que criou o vírus que apagou a tabela de alocação de arquivos do seu disco rígido não visava você ou o seu computador especificamente. Nem será motivo de alento saber que o problema com o vírus será provavelmente sempre nosso. Mas conhecer um pouco do histórico dos vírus de computador e como atuam pode ajudar a proteger melhor o seu sistema contra esses ataques.

Antecedentes dos vírus

Os pesquisadores de vírus identificaram alguns programas que serviram como precursores dos vírus, ou que incorporavam recursos atualmente associados a software de vírus. O educador e pesquisador canadense, Robert M. Slade, traça a linhagem dos vírus desde os utilitários com objetivos específicos usados para recuperar espaço em disco, ocupados por arquivos

que não eram utilizados, e executar outras tarefas úteis nos computadores ligados em rede mais antigos. Slade relata que os cientistas de computadores em um departamento de pesquisa da Xerox Corporation chamavam programas como esses de “vermes”, um termo usado depois que os cientistas notaram “orifícios” em mapas de memória de computador impressos, que eram semelhantes aos produzidos por vermes que os tivessem perfurado. O termo ainda é utilizado para descrever programas que se reproduzem, mas não alteram software host.

Uma forte tradição acadêmica de pregar peças através de computadores é a explicação mais provável do desvio da atenção dos programas utilitários em direção a usos mais destrutivos das técnicas de programação encontradas nos softwares “vermes”. Os estudantes de informática, para testar as suas habilidades programáticas, constroem programas “vermes” travessos e desencadeiam-nos para “lutar” entre si, competindo para ver qual programa “sobreviveria” aos rivais. Esses mesmos estudantes também encontraram utilidades para programas “vermes” nas peças pregadas em colegas confiantes.

Alguns desses estudantes logo descobriram que poderiam usar certos recursos do sistema operacional do computador host para conceder-lhes acesso não autorizado aos recursos do computador. Outros se aproveitaram de usuários que tinham relativamente pouco conhecimento de computadores para substituir seus programas — escritos com objetivos específicos — por utilitários inócuos ou comuns. Esses usuários simples executariam esses utilitários como se fossem os softwares usados rotineiramente e descobririam que seus arquivos foram apagados, suas senhas de contas roubadas ou sofreriam outras conseqüências desagradáveis. Esses programas do tipo “cavalo de Tróia” ou “troianos”, assim chamados por sua semelhança metafórica com o presente que os antigos gregos ofereceram à cidade de Tróia, continuam a ser uma ameaça significativa para os usuários de computadores atuais.

Vírus e a revolução dos PCs

O que agora conhecemos como um verdadeiro vírus de computador apareceu, inicialmente, segundo Robert Slade, logo depois que os primeiros computadores pessoais alcançaram o mercado de massa no início dos anos 80. Outros pesquisadores datam o advento dos programas de vírus em 1986, quando apareceu o vírus “Brain”. Não importa a data inicial, o vínculo entre a ameaça dos vírus e o computador pessoal não é acidental.

A nova distribuição em massa dos computadores significou que os vírus poderiam se espalhar em muito mais hosts que anteriormente, quando um número comparativamente pequeno de sistemas de grande porte altamente protegidos dominava o espaço da computação a partir de suas fortalezas em grandes corporações e universidades. Não havia necessidade dos usuários

individuais de computador, que compravam PCs, adotarem medidas de segurança sofisticadas utilizadas para proteger dados sensíveis nesses ambientes. Mais particularmente, os criadores de vírus acharam relativamente mais fácil explorar algumas tecnologias de PC para serem usadas em seus próprios objetivos.

Vírus de setor de inicialização

Os PCs antigos, por exemplo, eram inicializados ou carregavam os seus sistemas operacionais a partir de disquetes. Os autores do vírus Brain descobriram que poderiam substituir os seus programas pelo código executável presente no setor de inicialização de cada disquete formatado com o MS-DOS da Microsoft, incluindo ou não os arquivos de sistema. Com isso, os usuários carregavam o vírus na memória sempre que iniciavam seus computadores com qualquer disquete formatado em suas unidades de disco. Uma vez colocado na memória, um vírus poderia se reproduzir em setores de inicialização de outros disquetes ou discos rígidos. Aqueles que inadvertidamente carregaram o vírus Brain a partir de um disquete infectado se encontraram lendo uma “propaganda” substituto para uma companhia de consultoria de informática no Paquistão.

Com essa propaganda, o Brain foi pioneiro de outro recurso característico dos vírus modernos: a carga explosiva. Essa carga é a “piada” ou comportamento destrutivo que, se for ativado, causa efeitos que variam de mensagens desagradáveis a destruição de dados. É a característica do vírus que chama mais atenção — muitos autores de vírus agora escrevem-nos especificamente para colocar sua carga explosiva no maior número possível de computadores.

Durante algum tempo, os descendentes sofisticados desse primeiro vírus de setor de inicialização representaram a maior ameaça para os usuários de computador. Variações de vírus de setor de inicialização também infectam o Registro de inicialização principal (MBR), que armazena as informações sobre partição, das quais o computador necessita para saber onde encontrar cada uma das partições do seu disco rígido e o setor de inicialização.

Numa perspectiva realista, quase todas as etapas do processo de inicialização, da leitura do MBR à carga do sistema operacional, estão vulneráveis à sabotagem por vírus. Alguns dos mais tenazes e destrutivos vírus ainda incluem a habilidade para infectar o setor de inicialização do seu computador ou do MBR no seu repertório de truques. Entre outras vantagens, a carga durante a inicialização pode dar a oportunidade ao vírus de fazer o seu trabalho antes que o seu software antivírus possa ser executado.

Mas os vírus do setor de inicialização e do MBR têm uma fraqueza particular: podem se espalhar através de disquetes ou de outra mídia removível, mantendo-se ocultos na primeira trilha do espaço do disco. Como poucos usuários trocam disquetes e como a distribuição de softwares agora baseia-se em outras mídias, como CD-ROMs, outros tipos de vírus eclipsaram recentemente a ameaça ao setor de inicialização. A popularidade dos discos de alta capacidade, como o Iomega Zip e outros discos semelhantes da Syquest e outras empresas podem causar uma ressurgência. Vírus infectantes de arquivos

Vírus infectantes de arquivos

Mais ou menos ao mesmo tempo em que os autores do vírus Brain encontraram vulnerabilidades no setor de inicialização do DOS, outros criadores de vírus descobriram como usar o software existente para ajudá-los a replicar os seus inventos. Um exemplo antigo desse tipo de vírus apareceu em computadores na Universidade de Lehigh na Pensilvânia. O vírus infectava parte do interpretador de comando DOS, COMMAND.COM, que costumava ser usado para se carregar na memória. Uma vez carregado, propagava-se por outros arquivos COMMAND.COM não infectados sempre que um usuário digitasse algum comando DOS padrão que envolvesse acesso ao disco. Isso limitava a sua propagação aos disquetes que continham, normalmente, um sistema operacional completo.

O vírus posteriores rapidamente ultrapassaram essa limitação, à vezes com programas bem mais inteligentes. Os criadores de vírus podem, por exemplo, fazer com que os vírus adicionem o seu código no início de um arquivo executável, a fim de que, quando os usuários iniciarem um programa, o código do vírus é executado imediatamente, em seguida, transfere o controle de volta para o software legítimo, que é executado como se nada de incomum tivesse acontecido. Uma vez ativado, o vírus “fisga” ou “captura” as solicitações que o software legítimo faz ao sistema operacional e substitui as suas respostas. Especificamente, os vírus mais inteligentes podem, até mesmo, subverter as tentativas de limpá-los da memória capturando a seqüência de teclado CRTL+ALT+DELETE para uma reinicialização a quente, em seguida, produziam um reinício falso. Às vezes, somente uma indicação externa que algo no sistema estava errado — antes que qualquer carga explosiva detonasse — isto é, uma pequena modificação no tamanho de arquivo do software legítimo infectado.

Vírus de “atuação furtiva”, mutantes, criptografados e polimorfos

Discretos como devem ser, as alterações no tamanho de arquivo e outras evidências esparsas de uma infecção por vírus geralmente fornecem à maioria dos softwares antivírus pistas suficientes para localizar e remover o código ofensivo. Contudo, um dos maiores desafios para o criador de vírus é encontrar os modos de ocultar o seu trabalho. Os disfarces mais antigos se

constituíam em uma mistura de programação inovadora e revelações óbvias. O vírus Brain, por exemplo, redirecionava as solicitações de visualização de um setor de inicialização do disco para fora da localização real do setor infectado, enviando-a para a nova localização dos arquivos de inicialização deslocada pelo vírus. Essa capacidade de "atuação furtiva" habilitava este e outros vírus a ocultar-se das técnicas de busca tradicionais.

Como os vírus precisavam evitar reinfectar continuamente os sistemas host — isso iria aumentar rapidamente o tamanho de um arquivo infectado em proporções facilmente detectáveis ou consumiriam recursos de sistema suficientes que apontariam uma origem óbvia — seus autores também necessitavam instruí-los para deixar certos arquivos intocados. Eles abordaram esse problema fazendo com que o vírus escrevesse uma "assinatura" de código que marcaria os arquivos infectados com o sinal de software equivalente a "não perturbe". Embora esse procedimento evitasse que o vírus fosse revelado imediatamente, abriu caminho para que os softwares antivírus usassem também assinaturas de código para encontrar os vírus.

Em resposta, os criadores de vírus encontraram maneiras de esconder as assinaturas de código. Alguns vírus "mudariam" ou escreveriam assinaturas de código diferentes a cada nova infecção. Outros criptografaram a maioria das assinaturas de código ou o vírus em si, deixando apenas alguns bytes para serem usados como uma chave para a descodificação. Os novos vírus mais sofisticados empregaram a atuação furtiva, mutação e criptografia para aparecer em quase todas as variedades não detectáveis de novas formas. A localização desses vírus "polimorfos" precisavam da atuação de engenheiros de software para desenvolverem técnicas de programação muito elaboradas a fim de criar softwares antivírus.

Vírus de macro

Em torno de 1995, a guerra contra os vírus chegou a uma pausa. Novos vírus apareceram continuamente, ajudados em parte pela disponibilidade dos kits de vírus já prontos que habilitaram algumas pessoas que não eram programadores a criar um novo vírus instantaneamente. A maioria dos softwares antivírus existentes, contudo, podia ser facilmente atualizada para detectar e remover as variações do novo vírus, que consistiam basicamente de pequenos ajustes finos em modelos bem conhecidos.

Mas 1995 presenciou também o aparecimento do vírus Concept, que representou uma nova e surpreendente virada na história dos vírus. Antes do Concept, a maioria dos pesquisadores de vírus pensavam que os arquivos de dados — o texto, a planilha eletrônica ou documentos de desenho criados pelo software utilizado — eram imunes às infecções. Acima de tudo, os vírus são programas e, como tal precisavam ser executados da mesma forma que os softwares executáveis para poder causar danos. Por outro lado, os arquivos de dados, armazenavam simplesmente as informações digitadas quando o software era utilizado.

Essa distinção desapareceu quando a Microsoft começou a adicionar recursos de macro no Word e Excel, os seus principais aplicativos do conjunto Office. Usando essa versão despojada da sua linguagem Visual BASIC incluída no conjunto, os usuários podiam criar modelos de documentos que formatariam e incluiriam outros recursos aos documentos criados com o Word e Excel. Os criadores de vírus aproveitaram a oportunidade que isto apresentava para ocultar e espalhar os vírus em documentos que você, o usuário, criou.

A explosão da popularidade dos softwares de Internet e de correio eletrônico, que permitiu aos usuários anexar arquivos a mensagens, assegurou que os vírus de macro seriam difundidos muito rápido e amplamente. Em um ano, os vírus de macro tornaram-se as ameaças mais potentes jamais vistas.

Dentro do limite

Os softwares destrutivos começaram a introduzir-se até mesmo em áreas que se pensava estarem completamente fora dos limites de infecção. Os usuários do cliente mIRC Internet Relay Chat, por exemplo, relataram ter encontrado vírus construídos a partir da linguagem de script mIRC. Os vírus de script são enviados como texto simples, o que normalmente os impediria de serem infectados, porém as versões mais antigas do software de cliente mIRC interpretavam as instruções codificadas no script para executar ações indesejadas no computador do destinatário. Os fornecedores decidiram rapidamente desativar esse recurso nas versões atualizadas do software, mas o incidente com o mIRC ilustra a regra geral que estabelece que onde há um modo de explorar uma brecha na segurança de um software, alguém a encontrará e usará.

Alguns criadores de vírus fazem-no somente pela emoção que isso possa produzir ou para ganhar notoriedade em seu grupo. Outros, ainda, para se vingar de funcionários ou de pessoas que eles pensam os terem maltratado. Não importam os motivos, eles continuam a desenvolver novas maneiras de lhe causar problemas.

Como proteger o sistema

O software antivírus da Network Associates já lhe fornece uma importante proteção contra infecções e danos aos seus dados, mas este software é apenas uma parte das medidas de segurança que você deve tomar para proteger seus dados. A maioria das medidas são de bom comum — a verificação de discos recebidos de origem desconhecida ou questionável, usando um software antivírus ou algum tipo de utilitário de verificação, é sempre uma boa idéia. Os programadores destrutivos chegaram até a imitação de programas, que você acredita estarem protegendo o seu computador, apresentando-os com uma aparência familiar, porém com objetivos que estão longe de serem amistosos. A Network Associates inclui o VALIDATE.EXE, um utilitário de verificação, em suas distribuições para impedir esse tipo de manipulação, mas nem ele nem o software antivírus podem detectar quando alguém substitui um de seus utilitários comerciais ou shareware por um programa do tipo cavalo de Tróia ou um outro destrutivo.

O acesso à Internet e à Web apresenta os seus próprios riscos. É uma necessidade colocar uma barreira de proteção de primeira linha para a sua rede e implementar outras medidas de segurança quando atacantes inescrupulosos podem penetrar em sua rede a partir de quase todos os pontos do mundo, para roubar dados sensíveis ou implantar códigos destrutivos. Você também deve assegurar que a sua rede não esteja acessível a usuários não autorizados e que tenha sido implementado um programa em seu local de trabalho para ensinar e reforçar os padrões de segurança.

Para aprender mais sobre a origem, o comportamento e outras características dos vírus, consulte a Biblioteca de informações sobre vírus mantida no site da Web da Network Associates. Alguns produtos da Network Associates incluem ainda uma Lista de vírus que também cataloga todos os vírus que o programa pode detectar e resume as informações sobre os seus tamanhos, tipos de infecção tentadas e se o produto pode removê-los dos arquivos.

A Network Associates pode fornecer-lhe outros softwares do conjunto Total Virus Defense (TVD), a mais completa solução antivírus disponível, e Total Network Security (TNS), o conjunto de segurança de rede mais avançado da indústria. A Network Associates os apóia com suporte amplo, treinamento e uma rede mundial de equipes de pesquisa e desenvolvimento. Entre em contato com o seu representante da Network Associates ou visite o site da Web da Network Associates em **http://www.nai.com**, para saber como usar os recursos avançados da Total Virus Defense em seu sistema.

Como contactar a Network Associates

Atendimento ao cliente

Para encomendar produtos ou obter informações sobre produtos, entre em contato com o Departamento de Atendimento ao Cliente da Network Associates no telefone (011) 550-51009 ou escreva para os seguintes endereços:

Network Associates, Inc.
Rua Geraldo Flauzino Gomes 78-cj.
São Paulo, SP 04575-060
Brasil

Suporte técnico

A Network Associates é famosa pela dedicação à satisfação do cliente. Mantemos essa tradição tornando o nosso site da World Wide Web um recurso valioso para a obtenção de informações sobre assuntos relativos a suporte técnico. Encorajamos os nossos clientes a fazer desta a sua primeira parada para obter respostas a perguntas freqüentes, atualizações do software da Network Associates e acesso a novidades e informações sobre vírus..

World Wide Web	http://www.nai.com

Se você não encontrar o que precisa ou não tiver acesso à Web, experimente um de nossos serviços automatizados.

Sistema Automatizado de Resposta via Voz e Fax	00 1 (408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	palavra-have MCAFEE

Se os serviços automatizados não contiverem as respostas necessárias, entre em contato com a Network Associates através de um dos seguintes telefones, de segunda a sexta, das 6:00 às 18:00, Hora do Pacífico.

Para clientes com licença corporativa:

Tel:	00 1 (408) 988-3832
Fax	00 1 (408) 970-9727

Para clientes com licença para revenda:

Tel:	00 1 (972) 278-6100
Fax	00 1 (408) 970-9727

Para fornecer as respostas que você precisa de maneira rápida e eficiente, a equipe de suporte técnico da Network Associates precisa de algumas informações sobre o seu computador e o software. Tenha estas informações disponíveis antes de ligar:

- Nome do produto e número da versão
- Marca e modelo do computador
- Qualquer hardware ou periféricos adicionais conectados ao seu computador
- Tipo de sistema operacional e números das versões
- Tipo e versão da rede, se for aplicável
- Conteúdo do AUTOEXEC.BAT, CONFIG.SYS, script de LOGIN do seu sistema e o NOTES.INI
- Etapas específicas para reproduzir o problema.

Treinamento da Network Associates

Para obter informações sobre planejamento de treinamento no local para qualquer produto da Network Associates, ligue para 00 1 (800) 338-8754.

Informações sobre contato internacional

Para entrar em contato com a Network Associates fora dos Estados Unidos, use os endereços e telefones abaixo.

Network Associates Australia

Level 1, 500 Pacific Highway

St. Leonards, NSW 2065

Austrália

Tél. : 61-2-9437-5866

Fax : 61-2-9439-5166

Network Associates Canada

139 Main Street, Suite 201

Unionville, Ontario

Canadá L3R 2G6

Tél. : (905) 479-4189

Fax : (905) 479-4540

Network Associates Deutschland GmbH

Industriestrasse 1

D-82110 Germering

Alemanha

Tél. : 49 8989 43 5600

Fax : 49 8989 43 5699

Network Associates International B.V.

Gatwickstraat 25

1043 GL Amsterdam

Paises Baixos

Tél. : 31 20 586 6100

Fax : 31 20 586 6101

NA Network Associates Oy

Kielotie 14B

01300 Vantaa

Finland

Tél. : 358 9 836 2620

Fax : 358 9 836 26222

Network Associates France S.A.

50 rue de Londres

75008 Paris

France

Tél. : 33 1 44 908 737

Fax : 33 1 45 227 554

Network Associates Hong Kong

19/F, Matheson Centre

3 Matheson Street

Causeway Bay

Hong Kong

Tél. : 852-2832-9525

Fax : 852-2832-9530

Network Associates International Ltd.

Minton Place, Victoria Street

Windsor, Berkshire

SL4 1EG

Reino Unido

Tél. : 44 (0)1753 827500

Fax : 44 (0)1753 827520

Network Associates Japan, Inc.
Toranomon 33 Mori Bldg.
3-8-21 Toranomon
Minato-Ku, Tokyo 105-0001
Japão
Tél. : 81 3 5408 0700
Fax : 81 3 5408 0780

Network Associates Korea
135-090, 18th Floor, Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Séoul, República de Coreia
Tél. : 82-2-555-6818
Fax : 82-2-555-5779

Network Associates Portugal
Rua Gen. Ferreira Marines, 10-6 C
1495 ALGÉS
Portugal
Tél. : 351 1 412 1077
Fax : 351 1 412 1488

Network Associates South East Asia
78 Shenton Way
#29-02
Singapore 079120
Tél. : 65-222-7555
Fax : 65-220-7255

Network Associates Sweden
Datavägen 3A, box 59678
S-175 26 Järfälla
Suécia
Tel.: 46 8 580 100 02
Fax: 46 8 580 100 05

Network Associates Srl
Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italie
Tél. : 39 (0)2 9214 1555
Fax : 39 (0)2 9214 1644

Network Associates Latin America
150 S. Pine Island Road, Suite 205
Plantation, Floride 33324
EUA
Tél. : (954) 452-1731
Fax : (954) 236-8031

Network Associates Brazil
Rue Geraldo Flauzino Gomes 78-cj.51
04575-060 Sao Paulo
Brasil
Tél. : 55 11 550 51009
Fax : 55 11 550 51006

Network Associates Spain
Orense, 36. 3a planta
28020 Madrid
Espanha
Tel.: 34 902 40 90 40
Fax: 34 902 40 10 10

Network Associates Switzerland
Baeulerwisenstrasse 3
8152 Glattbrugg
Suisa
Teléfono:41 1 808 99 66
Fax: 41 1 808 99 77

Sumário

Introdução ao VirusScan 1

O McAfee VirusScan para Windows 3.1*x* é a solução antivírus para computador de mesa mais avançada da Network Associates. A estratégia de proteção do VirusScan contém três componentes: varredura ao acessar, varredura por solicitação e varredura planejada.

O VirusScan monitora continuamente o seu sistema para buscar atividade viral usando o componente de varredura ao acessar, o VShield. Se um vírus for detectado, você poderá atuar automaticamente para removê-lo, mover os arquivos infectados para outra localização ou excluir os arquivos infectados.

O VirusScan também pode ser iniciado pelo usuário para examinar um arquivo, pasta, disco ou volume. Este é o componente de varredura por solicitação da estratégia de proteção do VirusScan.

A varredura planejada permite que você configure o VirusScan para realizar varreduras específicas em momentos ou intervalos predeterminados. Assim, é possível examinar áreas particularmente vulneráveis do sistema com freqüência ou executar uma varredura completa de todo o sistema enquanto não está sendo usado.

O VirusScan é um elemento importante de um programa de segurança extenso que inclui várias medidas de segurança, como backups regulares, proteção significativa por senha, treinamento e conscientização. Recomendamos que você configure e consinta em usar esse programa de segurança como uma medida preventiva para proteger o seu sistema contra infecções. Para obter dicas sobre a criação de um ambiente seguro, veja Apêndice B, “Evitando a infecção por vírus.”

Recursos principais

- A varredura certificada pela NCSA assegura a detecção de 100 por cento dos vírus encontrados “na natureza”. Veja os status de certificações no site da Web da National Computer Security Association em **http://www.NCSA.com**.
- O VShield, a varredura ao acessar do VirusScan, identifica vírus conhecidos e desconhecidos em tempo real durante o acesso, criação, cópia, renomeação e execução de um arquivo, e na inicialização do sistema.
- A varredura por solicitação oferece uma detecção, iniciada pelo usuário, de vírus de inicialização, de arquivo, com diversas partes, de atuação furtiva, criptografados e polimorfos localizados em arquivos, unidades de disco e disquetes.

- As varreduras do Code Trace™ , Code Poly™ e Code Matrix™ empregam tecnologias de propriedade da Network Associates para localizar e identificar os vírus com precisão.
- O VirusScan pode ser configurado para atuar automaticamente na detecção do vírus, incluindo registro, exclusão, isolamento ou limpeza. O VirusScan também pode ser configurado para emitir alertas e produzir relatórios para uma localização de servidor centralizada.
- O VirusScan inclui um programador de tarefas para configurar varreduras diárias, semanais ou mensais.
- As atualizações mensais das assinaturas de vírus e as atualizações de versão do produto estão incluídas na compra da licença de assinatura da Network Associates para assegurar as melhores taxas de detecção e remoção de infecções.

Como funciona a detecção de vírus

O VirusScan monitora o seu computador e pesquisa as características (seqüências de códigos) específicas de cada vírus conhecido. Se um vírus for detectado, o VirusScan atua da maneira na qual você o configurou. Para os vírus que são criptografados ou mutantes, o programa usa algoritmos de detecção que dependem de análise estatística, heurística e desassemblagem do código.

Quando eu devo examinar o sistema para detectar vírus?

A varredura por solicitação do VirusScan realizará exames automáticos do seu sistema sempre que você acessar, criar, copiar, renomear ou executar um arquivo, ou iniciar o sistema. Essa varredura também protege o sistema contra vírus quando você carrega ou faz download de arquivos em redes.

Para obter uma máxima proteção, você deveria usar também o recurso de varredura por solicitação do VirusScan para buscar vírus sempre que adicionar arquivos ao seu sistema. Se forem copiados arquivos de um disquete ou forem obtidos por download em um serviço online, o VirusScan deve ser executado para assegurar que não houve infeccção por vírus.

Examine ao inserir um disquete desconhecido

Sempre que você inserir um disquete desconhecido em sua unidade, examine-o antes de executar, instalar ou copiar os arquivos nele contidos.

Examine ao instalar ou fazer download de novos arquivos

Sempre que você instalar um software novo no disco rígido ou fizer download de arquivos executáveis de um serviço online, execute o VirusScan para verificar os arquivos antes de usá-los.

Examine regularmente

Execute varreduras por solicitação em seu sistema regularmente, com a freqüência de uma vez por dia até uma vez por mês, dependendo da suscetibilidade do sistema à infecção por vírus. Planeje varreduras das áreas mais vulneráveis do sistema para obter máxima segurança.

Instalando o VirusScan 2

Antes de iniciar

Siga as etapas abaixo antes de instalar o VirusScan para Windows 3.1*x*. Este procedimento irá minimizar o risco de espalhar vírus que já podem estar presentes no seu sistema.

1. Reveja os requisitos de sistema para o VirusScan.
2. Certifique-se de que o sistema esteja livre de vírus. Se você suspeitar que o sistema já está infectado, veja "Se há suspeita de vírus" na página 59, antes de iniciar a instalação.

Requisitos de sistema

- PC compatível com IBM com o Windows 3.1 instalado*x*; 386 ou superior
- 5MB de espaço no disco rígido
- 4MB de memória disponível (8MB recomendados).

Procedimento de instalação

Esta seção descreve o procedimento básico de instalação. Veja o Apêndice C, "Instalações compartilhadas" para obter informações sobre instalações compartilhadas.

NOTA: Se você suspeitar que o sistema já está infectado por um vírus, veja "Se há suspeita de vírus" na página 59, antes de instalar o VirusScan.

Siga estas etapas para instalar o VirusScan no seu sistema:

1. Inicie o Windows.
2. Faça o seguinte:
   - Se estiver instalando a partir de um disquete ou CD-ROM de instalação VirusScan, insira-o.
   - Se a instalação for a partir de arquivos obtidos por download de uma BBS ou de do site da Web da Network Associates, descompacte os arquivos, em um diretório, na sua unidade local ou de rede.
3. Escolha **Executar** no menu Arquivo.

- Se você estiver instalando a partir de um disquete, digite:

  ```
  x:\setup.exe
  ```

  onde *x* é a unidade que contém o disquete. Clique em **OK**.

- Se estiver instalando a partir de um CD-ROM, digite:

  ```
  x:\win\setup.exe
  ```

  onde *x* é a unidade que contém o CD-ROM. Clique em **OK**.

- Se estiver instalando a partir de arquivos obtidos por download, digite:

  ```
  x:\path\setup.exe
  ```

  onde **x:\path** é a localização dos arquivos. Clique em **OK**.

4. Aparece o contrato de licença para o VirusScan. Leia-o com atenção, em seguida, clique em **Sim** para continuar.
5. Quando aparecer a tela Bem-vindo, leia as informações nela contidas, em seguida, clique em **Avançar** para continuar.
6. Selecione o tipo de instalação:

   - **Típica** realiza uma instalação completa do VirusScan com as opções mais comuns.
   - **Compacta** instala o VirusScan com as mínimas opções necessárias.
   - **Personalizada** permite selecionar os componentes do VirusScan que você deseja instalar.

7. Escolha o diretório no qual o VirusScan será instalado.

   - Digite o nome de um diretório na caixa de texto mostrada, em seguida, clique em **Avançar**.
   - Clique em **Procurar** para navegar até um diretório específico, em seguida, clique em **Avançar**.

8. Quando for solicitado, reveja as suas configurações e clique em **Avançar** para continuar. Os arquivos do VirusScan são copiados para o disco rígido.
9. Você é avisado para inserir um disquete em branco na unidade A:. Siga as instruções na tela para criar um Disco de Emergência que ajudará a recuperar os arquivos no caso de uma infecção no setor de inicialização.

NOTA: Se você não quiser criar um Disco de Emergência agora, clique em **Cancelar**. O Disco de Emergência pode ser criado posteriormente, clicando-se duas vezes no ícone correspondente, no grupo de programas do VirusScan.

10. Clique em **Sim** para rever o arquivo de texto O Que Há de Novo para obter informações sobre os novos recursos do VirusScan.
11. Reveja as alterações feitas nos arquivos do seu sistema, em seguida, clique em **Avançar**.
12. Selecione **Sim** para reiniciar o computador, em seguida, clique em **Concluir**. O sistema é reiniciado. Todas as alterações são ativadas. O VirusScan entra agora em execução.

NOTA: Se você tiver cancelado a criação do Disco de Emergência na etapa 8, crie esse disco imediatamente. Veja "Criando um Disco de Emergência" na página 72 para obter mais informações.

Testando a sua instalação

O Arquivo de teste antivírus padrão da Eicar é o resultado de um esforço conjunto de fornecedores de programas antivírus do mundo inteiro para criar um padrão único através do qual os clientes possam verificar suas instalações de software antivírus.

Para testar a sua instalação, copie a linha seguinte no seu próprio arquivo e denomine-o EICAR.COM.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

NOTA: Certifique-se de que essa cadeia de caracteres aparece em uma única linha do arquivo atual.

Ao terminar, o arquivo terá 69 ou 70 bytes. Quando o VirusScan examinar esse arquivo, relatará a localização do vírus EICAR-STANDARD-AV-TEST-FILE. Independentemente do que o VirusScan relatar, ele não encontrou um vírus de fato. Em vez disso, detectou um arquivo que se destina a testar o seu recurso de detecção de vírus com sucesso.

Exclua o arquivo EICAR.COM ao terminar o teste da instalação para evitar que os usuários não avisados fiquem desnecessariamente alarmados.

Varredura ao acessar 3

O que é a varredura ao acessar?

A varredura ao acessar é um dos três componentes da estratégia de proteção usada pelo VirusScan para Windows 3.1*x*. (Os outros são a varredura por solicitação e a varredura planejada.)

A varredura ao acessar é feita pelo VShield, um programa residente na memória, que usa uma série de módulos VxD (driver de dispositivo virtual carregado dinamicamente) para fornecer uma proteção em tempo real ao seu sistema. Esse tipo de varredura ajuda a evitar a infeccção por vírus através da verificação automática de programas — como arquivos, diretórios, unidades de disco e qualquer mídia — ao serem acessados.

Neste capítulo, você encontrará os procedimentos para iniciar e configurar o VShield, o componente para varredura ao acessar do VirusScan.

Iniciando o VShield

O VShield, a varredura ao acessar do VirusScan, é um driver de dispositivo virtual. Como padrão, o VShield é ativado automaticamente sempre que você inicia o Windows e continua ativo em segundo plano durante a sessão do Windows.

Você pode ativar o VShield de uma das seguintes maneiras:

- Clique duas vezes no ícone do VShield na área de trabalho. Se o botão na extremidade esquerda da caixa de diálogo resultante contiver “Desativar”, o VShield estará em funcionamento. Se contiver “Ativar,” clique mo botão para ativar o VShield.
- Execute o VSHWIN.EXE, que pode ser encontrado no diretório de instalação.

Se, por alguma razão, o VShield não for ativado quando o Windows for iniciado, será necessário reconfigurá-lo para ser carregado na inicialização. Para obter informações sobre o modo de fazer isso, veja “Configurando a varredura ao acessar” na página 10.

Usando a janela Status do VShield

Quando o VShield é ativado, você pode usar a janela Status do VShield (Figura 3-1) para configurar as suas opções de varredura ou exibir o status dos arquivos examinados. Para exibir essa janela, clique duas vezes no ícone do VShield, na área de trabalho.

NOTA: Se você não vir esse ícone, execute o Gerenciador de Configuração (VSHCFG16.EXE) do VShield e selecione **Mostrar ícone na área de trabalho**.

Figura 3-1. Janela Status do VShield

A janela Status do VShield mostra o nome do último arquivo examinado, o número de arquivos examinados, infectados, limpos, excluídos e movidos.

Além disso, estão disponíveis as seguintes opções:

- **Desativar/Ativar** ativa ou desativa a varredura ao acessar durante a sessão atual do Windows.
- **Propriedades** configura as definições de detecção, ação e relatório da varredura ao acessar. Veja "Configurando a varredura ao acessar" na página 10 para obter mais informações.
- **Fechar** fecha a janela Status do VShield.

Configurando a varredura ao acessar

Use o Gerenciador de Configuração do VShield para configurar a varredura ao acessar. Você pode iniciá-lo de uma das seguintes maneiras:

- Selecione **Propriedades** na janela Status do VShield. Veja "Usando a janela Status do VShield" para obter mais detalhes sobre a exibição desta janela.
- Execute o VSHCFG16.EXE, que está no diretório de instalação (a localização padrão é **C:\Neta\Viruscan**).

Aparece o Gerenciador de Configuração do VShield mostrando a página Detecção (Figura 3-2).

Configurando a detecção do VShield

Use a página Detecção (Figura 3-2) para informar ao VShield quais itens devem ser examinados e quando a varredura deve ocorrer.

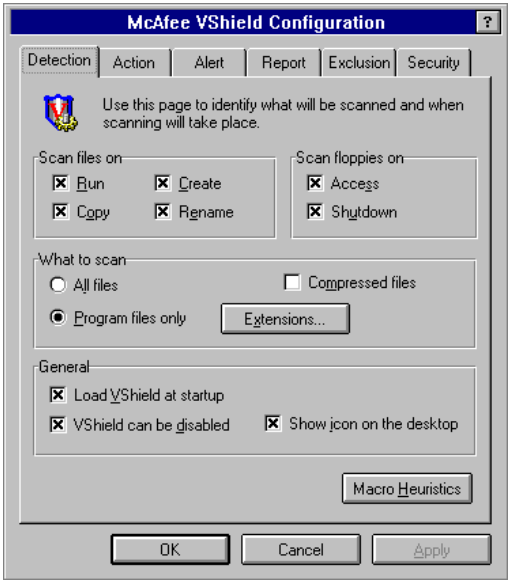

Figura 3-2. Gerenciador de Configuração do VShield (página Detecção)

Siga estas etapas para configurar as opções de detecção:

1. Selecione o(s) evento(s) que inicia(m) uma varredura do VShield.
   - **Executar** examina sempre que um arquivo for executado.
   - **Criar** examina sempre que um arquivo for criado.
   - **Copiar** examina sempre que um arquivo for copiado.
   - **Renomear** examina sempre que um arquivo for renomeado.

NOTA: Para obter máxima proteção, a Network Associates recomenda a seleção de todos os itens acima.

---

2. Selecione o(s) evento(s) que iniciam uma varredura de disquetes do VShield.

   - **Acessar** examina um disquete quando é acessado.
   - **Encerrar** examina a unidade de disco sempre que você fecha o sistema.

   NOTA: Para obter máxima proteção, a Network Associates recomenda a seleção de todos os itens acima.

   ---

3. Selecione os tipos de arquivos que o VShield deverá examinar.

   - **Todos os arquivos** examina todos os arquivos de qualquer tipo.
   - **Somente arquivos de programa** examina apenas os arquivos de sistema com determinadas extensões. Para alterar as extensões incluídas nessa lista, clique em **Extensões**.

     NOTA: As extensões padrão são .EXE, .COM, .DO? e .XL? (o ponto de interrogação representa um curinga). Essa lista produz uma varredura que verifica os arquivos de modelos e documentos (.DOC, .DOT, .XLS e .XLT) do Word e Excel, bem como os arquivos de programa.

   - **Arquivos compactados** examina os arquivos compactados com o PKLITE ou LZEXE.

4. Configure as preferências gerais.

   - **Carregar o Vshield ao iniciar** ativa a varredura ao acessar quando você inicia o Windows.
   - **VShield pode ser desativado** permite que a varredura ao acessar seja desativa.
   - **Mostrar ícone na área de trabalho** permite exibir a janela Status do VShield e selecionar as propriedades do VShield usando um ícone da área de trabalho.

     NOTA: A Network Associates recomenda a seleção de todos os itens. Contudo, os administradores de sistemas podem não querer ativar apenas **Carregar o VShield na inicialização** ao configurar o software do usuário. Para obter informações sobre os recursos de bloqueio do administrador do VShield, veja "Configurando a segurança do VShield" na página 21.

     ---

5. Se você quiser, clique em **Heurística de macro** para configurar a varredura heurística de macro. Essas opções permitem definir a varredura feita pelo VirusScan para limpar macros semelhantes a vírus nos documentos do Microsoft Word e Excel. Aparece a caixa de diálogo Configurações da varredura heurística (Figura 3-3).

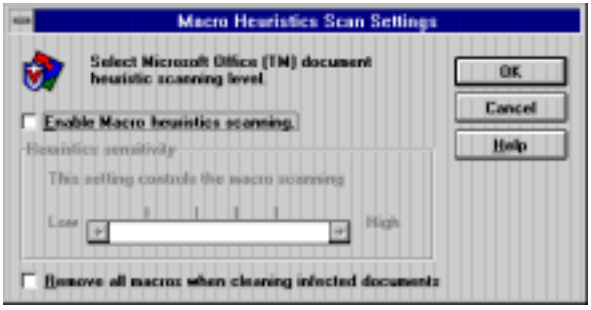

Figura 3-3. Caixa de diálogo Configurações da varredura heurística

   a. Ativa ou desativa a varredura heurística de macro. O padrão é ativada.

   b. Use o botão deslizante para configurar a precisão da varredura heurística de macro.

   c. Decida se o VirusScan removerá as macros quando estiver limpando os documentos infectados. Como padrão, o VirusScan remove as macros.

   d. Clique em **OK**.

NOTA: Se você mover o botão deslizante para a posição Alta *e* selecionar Remover todas as macros ao limpar documentos infectados, o VirusScan removerá as macros de todos os documentos do Word ou Excel que seja examinado — não somente as macros semelhantes a vírus.

---

6. Faça o seguinte:

   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração do VShield.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações, veja "Configurando a segurança do VShield" na página 21.

Configurando as ações do VShield

Use a página Ação (Figura 3-4) para informar ao VShield o que fazer se um vírus for detectado.

Figura 3-4. Gerenciador de Configuração do VShield (página Ação)

Siga estas etapas para configurar as definições da ação:

1. Na lista Quando um vírus for encontrado, escolha uma das seguintes ações:

   - **Solicitar ação ao usuário** faz com que o VShield pergunte o que vai fazer sempre que encontrar um vírus. As opções possíveis são:

     – **Limpar arquivo**.

     – **Excluir arquivo**.

     – **Eliminar arquivo**.

     – **Interromper o acesso**.

     – **Continuar o acesso**. Esta ação é recomendada para sistemas supervisionados.

   - **Mover arquivos infectados automaticamente** move cada arquivo infectado para uma pasta, que você escolhe. Especifique um caminho na caixa de texto Pasta de destino ou escolha **Procurar** para localizar uma pasta.

     O caminho da pasta pode ser relativo. Por exemplo, se você digitar `\Infectado` na caixa de texto, o VShield criará uma pasta chamada "Infectado" na unidade onde foi encontrado o arquivo infectado. Os arquivos infectados são movidos para essa pasta.

     NOTA: Se um arquivo infectado não puder ser limpo ou o VShield não tiver as permissões de acesso adequadas ao arquivo, o acesso será negado.

   - **Limpar arquivos infectados automaticamente** faz com o VShield limpe um arquivo infectado sem pedir permissão.

   - **Excluir arquivos infectados automaticamente** faz com que o VShield exclua um arquivo infectado sem pedir permissão. Em seguida, você deve restaurar uma cópia limpa do arquivo excluído a partir do backup.

   - **Negar acesso a arquivos infectados e continuar** impede que qualquer programa em seu sistema tenha acesso a um arquivo infectado até que você informe ao VShield o que fazer com esse arquivo. Esta ação é recomendada para os sistemas cuja varredura não é supervisionada.

2. Faça o seguinte:

   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciardor de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações, veja "Configurando a segurança do VShield" na página 21.

Configurando os alarmes do VShield

Use a página Alerta (Figura 3-5) para informar ao VShield qual método de alerta usar para alertá-lo e às outras pessoas, quando um vírus for detectado.

Figura 3-5. Gerenciador de Configuração do VShield (página Alerta)

Siga estas etapas para configurar os alertas do VShield:

1. Selecione **Enviar alerta de rede** para que o VShield envie alertas para um caminho de rede monitorado pelo NetShield, a solução de antivírus para servidor da Network Associates. Clique em **Procurar** para navegar até o diretório.

NOTA: Esse diretório deve conter o arquivo Alerta centralizado, CENTALERT.TXT. Para obter informações sobre Alerta centralizado, veja a documentação do NetShield.

2. Selecione **Soar alerta audível** e/ou **Exibir mensagem personalizada**. Você pode alterar a mensagem clicando na caixa e editando o texto.
3. Faça o seguinte:
   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar a janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações feitas, veja "Configurando a segurança do VShield" na página 21.

Configurando os relatórios do VShield

Use a página Relatório (Figura 3-6) para informar ao VShield como registrar as atividades do vírus e quais informações devem ser incluídas na entrada do registro.

Figura 3-6. Gerenciador de Configuração do VShield (página Relatório)

NOTA: O arquivo de registro é um arquivo de texto que pode ser exibido com qualquer editor de texto, como o Bloco de Notas.

Siga estas etapas para configurar as definições do relatório.

1. Selecione **Registrar no arquivo**, em seguida, execute uma das seguintes opções:
   - Digite um caminho e um nome de arquivo na caixa de texto
   - Escolha um caminho clicando em **Procurar**.
2. Limite o tamanho do arquivo de registro selecionando **Limitar tamanho do arquivo de registro em** e especifique um valor entre 10KB e 999KB.

   NOTA: O arquivo de registro padrão é **C:\Neta\Viruscan\VSHLOG.TXT**. O tamanho máximo do arquivo de registro padrão é 100KB.

3. Escolha as informações que devem ser incluídas no arquivo de registro. As opções incluem:
   - Detecção de vírus
   - Limpeza de vírus
   - Eliminação do arquivo infectado
   - Movimentação do arquivo infectado
   - Configurações da sessão
   - Resumo da sessão
   - Data e hora
   - Nome do usuário.

4. Faça o seguinte:

   - Clique em **Aplicar** para salvar as alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações feitas, veja "Configurando a segurança do VShield" na página 21.

Configurando as exclusões do VShield

Use a página Exclusão (Figura 3-7) para excluir itens das varreduras.

Figura 3-7. Gerenciador de Configuração do VShield (página Exclusão)

NOTA: A pasta **C:\Neta\Viruscan\Infectado** é automaticamente excluída.

Adicionando um item à lista de exclusão

Para adicionar um item na lista de exclusão, siga estas etapas:

1. Clique em **Adicionar** na página Exclusão. Aparece a caixa de diálogo Excluir item (Figura 3-8).

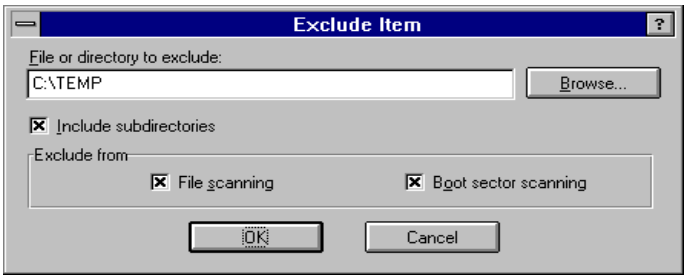

Figura 3-8. Caixa de diálogo Excluir item

2. Digite o caminho para o arquivo ou a pasta que deve ser excluída da varredura, ou clique em **Procurar** para localizar uma pasta.

NOTA: Você pode procurar somente as pastas. Para excluir um arquivo, digite manualmente o caminho e o nome do arquivo na caixa de diálogo Excluir item.

---

3. Selecione **Incluir subpastas** para excluir todas as subpastas contidas na pasta selecionada.
4. Se você quiser, exclua a pasta de uma varredura de arquivo ou de setor de inicialização selecionando a(s) caixa(s) adequada(s).
5. Clique em **OK**.
6. Faça o seguinte:

   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações feitas, veja “Configurando a segurança do VShield” na página 21.

Removendo um item da lista de exclusão

Para remover um item da lista, siga estas etapas:

1. Selecione o item, em seguida clique em **Remover**.
2. Faça o seguinte:
   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar a janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações feitas, veja "Configurando a segurança do VShield" na página 21.

Editando um item na lista de exclusão

Para editar um item existente na lista de exclusão, siga estas etapas

1. Selecione o item e clique em **Editar**.
2. Aparece a caixa de diálogo Excluir item (Figura 3-8 na página 20). Faça as suas alterações, em seguida, clique em **OK**.
3. Faça o seguinte:
   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações, veja "Configurando a segurança do VShield" na página 21.

Configurando a segurança do VShield

Use a página Segurança (Figura 3-9 na página 22) para bloquear e proteger por senha as configurações do VShield. Você deve usar esse recurso se for um administrador de sistemas e não quiser que os usuários comprometam a segurança alterando essas configurações.

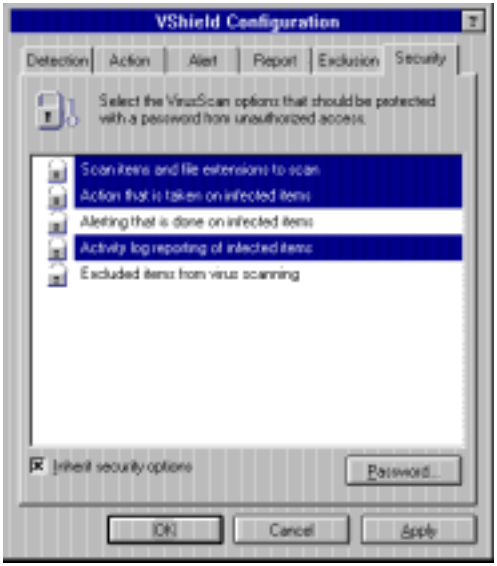

Figura 3-9. Gerenciador de Configuração do VShield (página Segurança)

Siga estas etapas para bloquear as configurações do VShield:

1. Selecione quais das seguintes configurações do VShield devem ser protegidas por senha:

   - **Itens de varredura e extensões de arquivo a serem examinadas**
   - **Ação tomada para os itens infetados**
   - **Alerta para os itens infectados**
   - **Relatório do arquivo de atividades sobre os itens infectados**
   - **Itens excluídos da varredura**.

   NOTA: Cada configuração protegida por senha será colocada em destaque e o cadeado à sua esquerda será fechado.

2. Clique em **Senha** para criar e alterar uma senha. Você será solicitado a digitar e confirmar a sua senha.

3. Faça o seguinte:

   - Clique em **Aplicar** para salvar as suas alterações sem sair do Gerenciador de Configuração.
   - Clique em **OK** para salvar as suas alterações e retornar à janela Status do VShield.
   - Clique em **Cancelar** para retornar à janela Status do VShield sem salvar as suas alterações.
   - Para bloquear e proteger por senha as suas alterações, veja "Configurando a segurança do VShield" na página 21.

Varredura por solicitação 4

O que é a varredura por solicitação?

A varredura por solicitação é um dos três componentes da estratégia de proteção usada pelo VirusScan para Windows 3.1*x*. (As outras são a varredura ao acessar e a planejada.)

A varredura por solicitação permite examinar itens específicos durante um trabalho, além de nova mídia ou arquivos específicos para determinar se o computador está infectado por vírus. O VirusScan detecta imediatamente vírus de inicialização, arquivo, com várias partes, furtivos, criptografados e polimorfos conhecidos, que estejam em arquivos, unidades de disco e disquetes.

Este capítulo abrange os procedimentos necessários para iniciar o componente por solicitação do VirusScan, bem como as etapas necessárias para configurar e personalizar as funções.

Iniciando o VirusScan

Para iniciar o VirusScan, clique duas vezes no ícone correspondente, no grupo de programas do VirusScan. Ao ser carregado, o VirusScan executa uma autoverificação de seus arquivos de programa e da memória do computador para assegurar que não contêm vírus.

Uma vez concluída a autoverificação, aparece a janela principal do VirusScan (Figura 4-1 na página 26), mostrando a página Detecção.

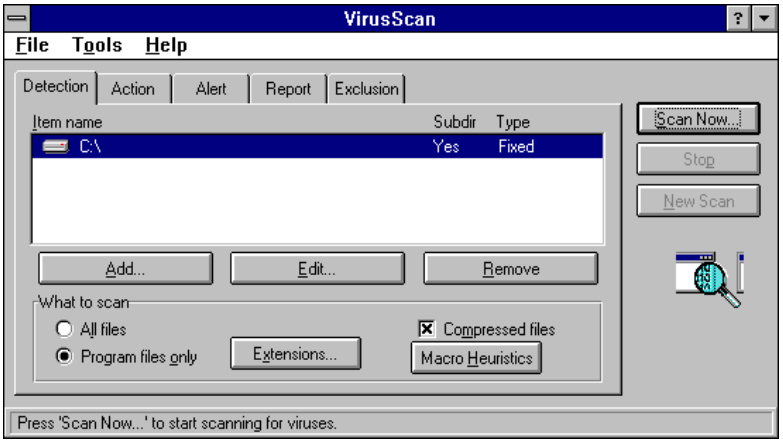

Figura 4-1. Janela principal do VirusScan Main (página Detecção)

NOTA: Se houver uma falha na autoverificação ou o VirusScan sair do Windows durante o carregamento, desligue o computador e execute o programa de linha de comando do VirusScan a partir do Disco de Emergência. Veja "Criando um Disco de Emergência" na página 72 para obter instruções sobre a criação de um Disco de Emergência.

Na janela principal, são estabelecidas as configurações da varredura, é iniciada a varredura por solicitação, exibido o registro de atividades e a Lista de vírus, podem ser impressos os relatórios e visualizados os resultados da varredura.

Configurando a varredura por solicitação

Os recursos configuráveis do VirusScan podem ser acessados através de cinco páginas com guias. As seguintes seções explicam como usar essas páginas para configurar o VirusScan de acordo com as suas necessidades.

Configurando a detecção do VirusScan

Antes de examinar ou limpar o sistema com o VirusScan, você deve usar a página Detecção para especificar os itens que serão incluídos na varredura.

Para selecionar as unidades de disco, diretórios ou arquivos a serem examinados, siga estas etapas:

1. Inicie o VirusScan. Aparece a janela principal do VirusScan, mostrando a página Detecção (Figura 4-1).

2. Para adicionar um item à lista, clique em **Adicionar**. Aparece a caixa de diálogo Adicionar item de varredura (Figura 4-2). (A unidade C: é selecionada como padrão.)

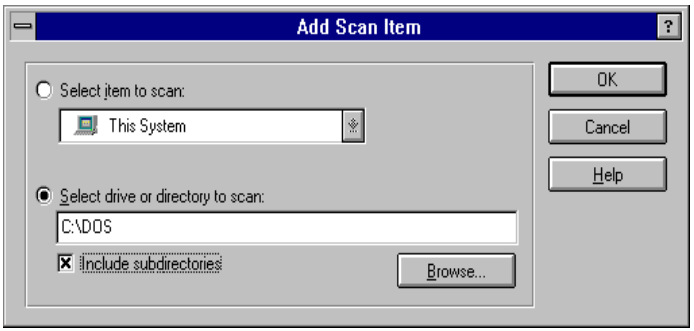

Figura 4-2. Caixa de diálogo Adicionar item de varredura

3. Para adicionar grupos de unidades de disco ou mídia, escolha **Selecionar item para examinar**, em seguida, escolha uma das seguintes opções:

   – **Este sistema** examina todos os volumes fixos, removíveis e de rede conectados ao computador.

   – **Toda a mídia removível** examina toda a mídia local removível, como disquetes e CR-ROMs.

   – **Todos os discos fixos** examina todos os discos rígidos locais.

   – **Todas as unidades de rede** examina todos os volumes de rede mapeados.

NOTA: Serão examinados todos os diretórios e subdiretórios nas localizações especificadas.

---

4. Para adicionar uma unidade de disco, arquivo ou pasta, selecione **Selecionar unidade ou pasta para examinar**, em seguida, escolha uma das seguintes opções:

   – Clique na caixa de texto e digite o caminho do item que será examinado.

   – Clique em **Procurar** para navegar até o arquivo, unidade ou pasta.

5. Se quiser, selecione Incluir subdiretórios para examiná-los na unidade ou pasta escolhida na Passo 4.

6. Clique em **OK**. Os itens selecionados aparecem na Lista de seleções.

7. Para remover um item da lista a ser examinada, selecione-o e clique em **Remover**. O item desaparecerá da lista.

8. Selecione os tipos de arquivos nos quais o VirusScan deve procurar vírus.

   - Selecione **Todos os arquivos** para examinar todos os arquivos, de qualquer tipo. O resultado disso é uma varredura mais completa, porém mais lenta.
   - Selecione **Somente arquivos de programas** para examinar apenas os arquivos com determinadas extensões. Para editar extensões nessa lista, clique em **Extensões**.

     NOTA: As extensões padrão são .EXE, .COM, .DO? e .XL? (o ponto de interrogação representa um coringa). Essa lista examina os arquivos de documentos e modelos do Word e Excel (.DOC, .DOT, .XLS e .XLT), bem como os arquivos de programas.

   - Selecione **Arquivos compactados** para examinar o conteúdo dos arquivos compactados com PKLITE ou LZEXE.

9. Se você quiser, clique em **Heurística de macro** para definir a varredura usada pelo VirusScan para limpar macros que possam conter vírus nos documentos do Microsoft Word e Excel. Aparece a caixa de diálogo Configurações da varredura heurística (Figura 4-3).

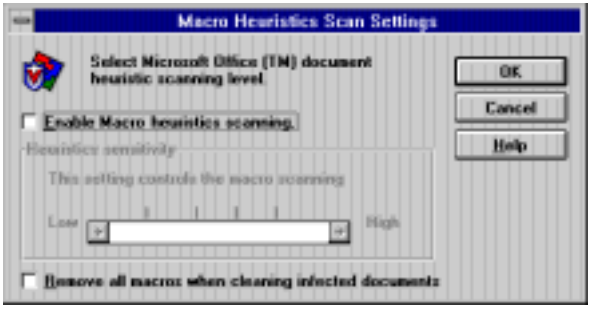

Figura 4-3. Caixa de diálogo Configurações da varredura heurística

   a. Ativa ou desativa a varredura heurística de macro. O padrão é ativada.

   b. Use o botão deslizante para definir a precisão da varredura.

   c. Decida se o VirusScan removerá as macros quando estiver limpando os documentos infectados. Como padrão, o VirusScan remove as macros.

d. Clique em **OK**.

NOTA: Se você mover o botão deslizante para Alta *e* selecionar Remover todas as macros ao limpar documentos infectados, o VirusScan remove as macros de qualquer documento do Word ou Excel examinado — não somente as macros semelhantes a vírus.

---

10. Faça o seguinte:

- Para salvar estas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
- Para continuar a configuração do VirusScan, selecione outra página.
- Para iniciar a varredura imediatamente usando as definições atuais, clique em **Examinar**.
- Para bloquear e proteger por senha estas configurações, veja "Usando Proteção por Senha" na página 39.

Configurando as ações do VirusScan

Siga estas etapas para informar ao VirusScan como atuar quando for detectado um vírus:

1. Inicie o VirusScan e selecione a página Ação. Aparece a janela principal do VirusScan, mostrando a página Ação (Figura 4-4).

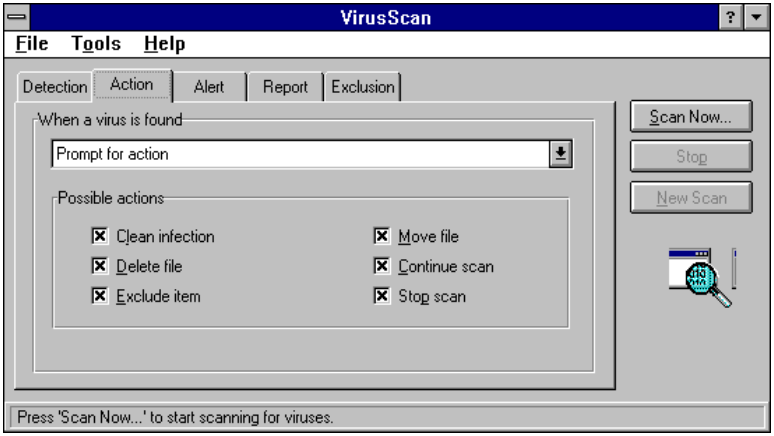

Figura 4-4. Janela principal do VirusScan (página Ação)

2. Selecione uma das seguintes ações:

   - **Solicitar ação** faz o VirusScan perguntar como irá atuar ao encontrar um vírus. Use esta opção se houver alguém próximo ao computador durante a varredura.

     NOTA: Escolha as ações disponíveis para o usuário, marcando as caixas de seleção adequadas em Ações possíveis.

   - **Mover arquivos infectados para um diretório** informa ao VirusScan para mover automaticamente os arquivos para um diretório de quarentena.

     NOTA: Você deve especificar o diretório para o qual os arquivos devem ser movidos. O diretório padrão é **\infectado**. A menos que seja especificado o caminho completo (por ex., **C:\mystuff\infectado**), o VirusScan criará o diretório no nível raiz da unidade onde o vírus foi encontrado (por ex., **C:\infectado**).

   - **Limpar arquivo infectado** informa ao VirusScan para limpar automaticamente os vírus dos arquivos infectados.

   - **Excluir o arquivo infectado** informa ao VirusScan para excluir automaticamente os arquivos infectados que forem encontrados.

     NOTA: Esta opção remove permanentemente os arquivos infectados do seu sistema. Você deve restaurar os arquivos excluídos a partir de backups limpos.

   - **Continuar a varredura** informa ao VirusScan para ignorar os arquivos infectados e continuar a varredura. O VirusScan não atua ao detectar um vírus.

3. Faça o seguinte:

   - Para salvar as suas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.

   - Para continuar a configurar o VirusScan, selecione outra página.

   - Para iniciar a varredura imediatamente usando as configurações atuais, clique em **Examinar**.

- Para bloquear e proteger por senha essas configurações, veja “Usando Proteção por Senha” na página 39.

Configurando os alertas do VirusScan

O VirusScan pode ser configurado para enviar um alerta ao detectar uma infecção por vírus. Use o procedimento abaixo para configurar os recursos de alerta do VirusScan:

1. Inicie o VirusScan e selecione a página Alerta. Aparece a janela principal do VirusScan (Figura 4-5) mostrando a página Alerta.

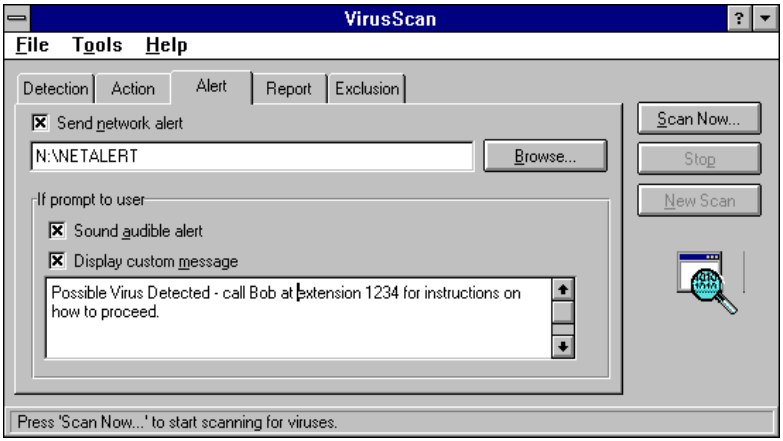

Figura 4-5. Janela principal do VirusScan (página Alerta)

2. Clique em **Enviar alerta de rede** se você quiser que o VShield envie alertas para um caminho de rede monitorado pelo NetShield, ou a solução antivírus de servidor da Network Associates. Clique em **Procurar** para navegar até o diretório.

NOTA: Esse diretório deve conter o arquivo Alerta centralizado, CENTALERT.TXT. Para obter informações sobre Alerta centralizado, veja a documentação do NetShield.

---

3. Se você selecionar **Solicitar ação** na página Ação, escolha **Soar alerta audível** e / ou **Exibir mensagem personalizada**. É possível alterar a mensagem clicando na caixa de texto para alterar o texto da mensagem.

4. Faça o seguinte:

   - Para salvar estas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
   - Para continuar a configurar o VirusScan, selecione outra página.
   - Para iniciar a varredura imediatamente usando as definições atuais, clique em **Examinar**.
   - Para bloquear e proteger por senha essas configurações, veja "Usando Proteção por Senha" na página 39.

Configurando relatórios do VirusScan

Siga estas etapas para configurar onde e como o VirusScan registra as suas atividades:

1. Inicie o VirusScan e clique na página Relatório. Aparece a janela principal do VirusScan, mostrando a página Relatório (Figura 4-6).

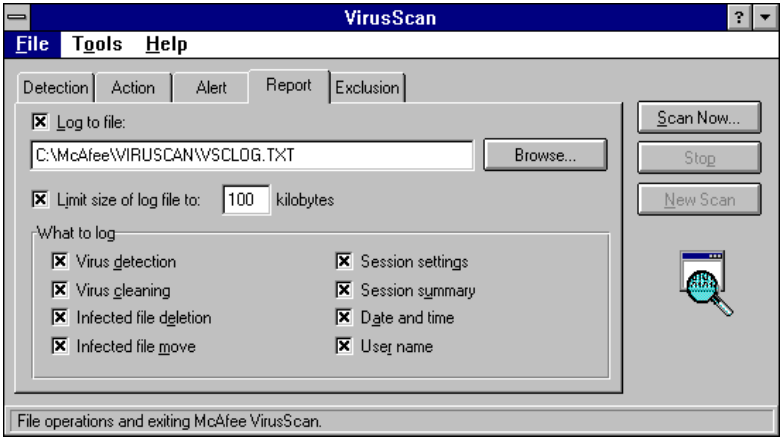

Figura 4-6. Janela principal do VirusScan (página Relatório)

2. Selecione **Registrar no arquivo**, em seguida, execute uma das seguintes opções:

   - Digite um caminho e um nome de arquivo na caixa de texto
   - Escolha um caminho clicando em **Procurar**.

3. Limite o tamanho do arquivo de registro selecionando **Limitar tamanho** e especifique um valor máximo.

NOTA: O arquivo de registro padrão é **C:\Neta\Viruscan\VSHLOG.TXT**. Esse é um arquivo de texto simples, que pode ser exibido com qualquer editor de texto (como o Bloco de Notas) ou escolhendo **Exibir registro de atividades** , no menu Arquivo.

---

4. Escolha as informações que devem ser incluídas no arquivo de registro. As opções incluem:

   - Detecção de vírus
   - Limpeza de vírus
   - Eliminação do arquivo infectado
   - Movimentação do arquivo infectado
   - Configurações da sessão
   - Resumo da sessão
   - Data e hora
   - Nome do usuário.

5. Faça o seguinte:

   - Para salvar estas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
   - Para continuar a configuração do VirusScan, selecione outra página.
   - Para iniciar a varredura imediatamente usando as configurações atuais, clique em **Examinar**.
   - Para bloquear e proteger por senha essas configurações, veja "Usando Proteção por Senha" na página 39.

Configurando as exclusões do VirusScan

A página Exclusão (Figura 4-7) permite configurar o VirusScan para que exclua arquivos, pastas ou unidades de suas varreduras.

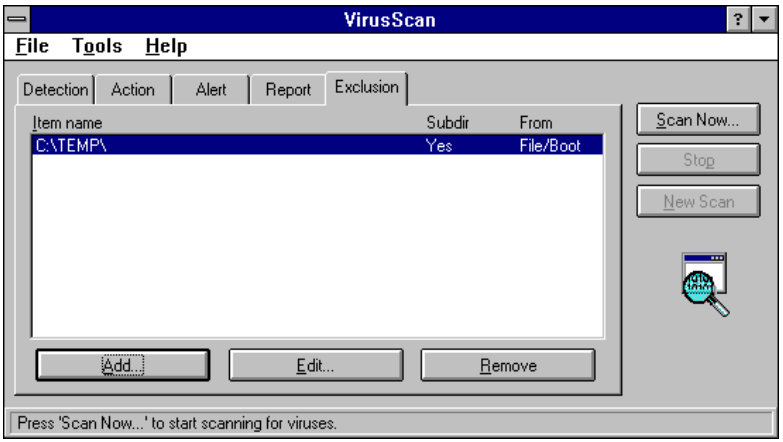

Figura 4-7. Janela principal do VirusScan (página Exclusão)

NOTA: A pasta **C:\Neta\Viruscan\Infectado** é automaticamente excluída.

Adicionando um item à lista de exclusão

Para adicionar um item na lista de exclusão, siga estas etapas:

1. Na página Exclusão, clique em **Adicionar**. Aparece a caixa de diálogo Excluir item (Figura 4-8).

Figura 4-8. Caixa de diálogo Excluir item

2. Digite o caminho item que será excluído ou clique em **Procurar** para navegar até ele. Pode ser excluído um arquivo, pasta ou um disco inteiro.
3. Selecione **Incluir subpastas** para que o VirusScan não examine as subpastas da pasta excluída da varredura.
4. Se preferir, exclua a varredura de arquivo de pasta ou a varredura de setor de inicialização marcando a(s) caixa(s) apropriada(s).
5. Clique em **OK**.
6. Faça o seguinte:
   - Para salvar essas seleções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
   - Para continuar a configuração do VirusScan, selecione outra página.
   - Para iniciar a varredura imediatamente usando as configurações atuais, clique em **Examinar**.
   - Para bloquear e proteger por senha essas configurações, veja "Usando Proteção por Senha" na página 39.

Removendo um item da lista de exclusão

Para remover um item da lista, siga estas etapas:

1. Na página Exclusão, selecione o item que deseja remover.
2. Clique em **Remover**.
3. Faça o seguinte:
   - Para salvar estas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
   - Para continuar a configuração do VirusScan, selecione outra página.
   - Para iniciar a varredura imediatamente usando as configurações atuais, clique em **Examinar**.
   - Para bloquear e proteger por senha essas configurações, veja "Usando Proteção por Senha" na página 39.

Editando um item na lista de exclusão

Para editar um item da lista de exclusões, siga estas etapas

1. Na pasta Exclusão, selecione o item que será editado.
2. Clique em **Editar**.

3. Aparece a caixa de diálogo Excluir item (Figura 4-8 na página 34). Faça as suas alterações, em seguida, clique em **OK**.

4. Faça o seguinte:

   - Para salvar estas opções em um arquivo de configurações, veja "Salvando as configurações da varredura" na página 36.
   - Para continuar a configuração do VirusScan, selecione outra página.
   - Para iniciar a varredura imediatamente usando as configurações atuais, clique em **Examinar**.
   - Para bloquear e proteger por senha essas configurações, veja "Usando Proteção por Senha" na página 39.

Salvando as configurações da varredura

O menu Arquivo do VirusScan contém duas opções para salvar as suas configurações:

- Salvar como padrão
- Salvar configurações.

Em cada um dos casos, as configurações são salvadas em um arquivo .VSC — um arquivo de texto de configuração que descreve as definições do VirusScan. O nome de cada variável é seguido por um sinal de igual (=) e por um valor que indica quais configurações foram selecionadas para o VirusScan.

As subseções seguintes explicam quando cada opção de salvamento deve ser utilizada.

Quando salvar como padrão

Se você quiser que o VirusScan use outra configuração ao salvar as suas definições padrão, escolha **Salvar como padrão**. As suas alterações são salvadas no arquivo DEFAULT.VSC.

Quando salvar as configurações

Se for necessária mais de uma configuração para o VirusScan — para examinar duas unidades de disco locais com definições distintas — escolha **Salvar configurações**. Você deverá especificar um nome para o novo arquivo .VSC, onde serão salvadas as novas configurações do VirusScan. Uma vez salvado o arquivo, pode ser usado clicando duas vezes em seu nome no Gerenciador de Arquivos do Windows.

NOTA: Pode ser necessário associar o arquivo .VSC ao VirusScan, na primeira vez que for utilizado. Veja as instruções na documentação do Windows.

Exibindo informações sobre vírus

A Lista de vírus é uma relação completa dos vírus detectados pelo VirusScan. Contém uma descrição dos vírus, os tipos, as características, o tamanho e o status da limpeza.

Exibindo a Lista de vírus

Para exibir e usar a Lista de vírus, siga estas etapas:

1. Inicie o VirusScan. Aparece a janela principal do VirusScan (Figura 4-1 na página 26).
2. Selecione **Lista de vírus** a partir do menu Ferramentas. A janela Lista de vírus (Figura 4-9) aparece.

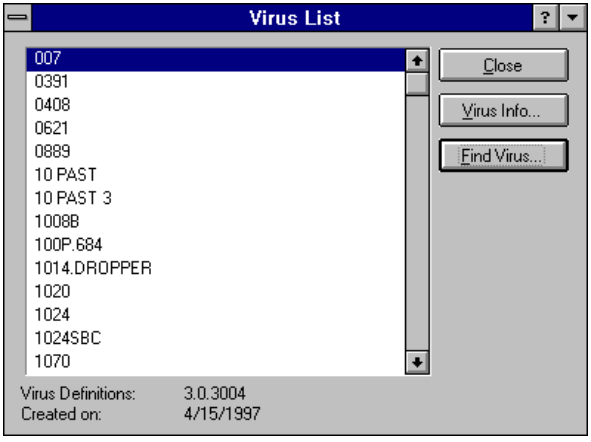

Figura 4-9. Janela Lista de vírus

3. Para visualizar informações sobre um vírus, siga uma das seguintes instruções:
   - Selecione-o a partir da lista e clique em **Informações sobre vírus**. A janela Informações sobre vírus (Figura 4-10 na página 38) aparece.

- Clique em **Localizar vírus** e digite o nome do vírus desejado na caixa de texto que aparece. Quando vir o vírus desejado na lista de vírus, feche a caixa de texto e clique em **Informações sobre vírus**. A janela Informações sobre vírus (Figura 4-10) aparece.

A janela Informações sobre vírus

A janela Informações sobre vírus (Figura 4-10) fornece informações detalhadas sobre o vírus selecionado na janela Lista de vírus.

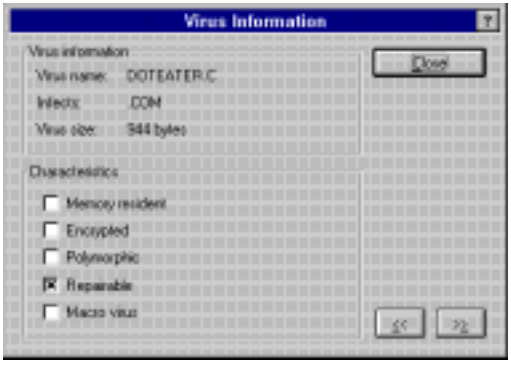

Figura 4-10. Janela Informações sobre vírus

A seção Informações sobre vírus da janela fornece informações básicas sobre o vírus:

- **Nome do vírus** é o nome do vírus.
- **Infecta** informa o que o vírus infecta, como arquivos de um tipo específico, o setor de inicialização ou o registro de inicialização master.
- **Tamanho do vírus** fornece o tamanho do vírus em bytes.

A seção Características descreve o comportamento do vírus selecionado:

- **Residente na memória** significa que o vírus é um programa residente na memória que age de forma similar a um TSR ou um driver de dispositivo, e permanece ativo na memória enquanto o computador estiver ligado.
- **Criptografado** significa que o vírus tenta escapar da detecção através de autocriptografia.
- **Polimorfo** significa que o vírus tenta escapar da detecção alterando sua estrutura interna ou suas técnicas de criptografia.
- **Reparável** significa que existe um removedor para o vírus.

- **Tamanho do vírus** indica quanto, em bytes, o vírus aumenta o tamanho de um arquivo infectado.

NOTA: O tamanho padrão para um vírus de MBR ou do setor de inicialização é 512 bytes.

Usando Proteção por Senha

Você pode proteger por senha as configurações do VirusScan para impedir alterações indesejadas. Os administradores de rede podem usar esta opção para impedir que usuários criem uma brecha na segurança através da alteração das configurações do VirusScan. Para utilizar proteção por senha, siga estas etapas:

1. Inicie o VirusScan. A janela principal do VirusScan aparece (veja Figura 4-1 na página 26).
2. Selecione Proteção por senha no menu Ferramentas. A caixa de diálogo Proteção por Senha aparece (Figura 4-11).

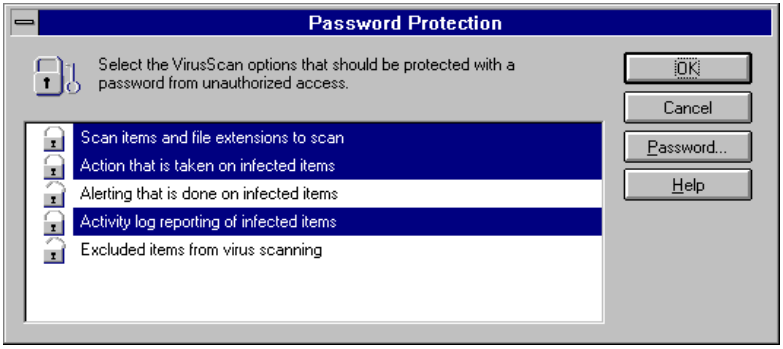

Figura 4-11. Caixa de diálogo Proteção por senha

3. Selecione os itens da lista que deseja proteger por senha.
4. Clique em**Senha** para inserir uma senha. Será solicitada a confirmação da senha.
5. Faça o seguinte:
   - Para salvar estas configurações e retornar para a janela Principal, clique em **OK**.
   - Para cancelar as suas alterações e retornar para a janela Principal, clique em **Cancelar**.

Varredura planejada 5

A varredura planejada é um dos três componentes da estratégia de proteção usada pelo VirusScan para Windows 3.1*x*. (Os outros são as varreduras ao acessar e por solicitação). A varredura planejada permite configurar o VirusScan para que inicie automaticamente a varredura em um horário predefinido. As varreduras podem ser realizadas uma vez, diariamente, semanalmente, mensalmente ou até a cada hora.

Neste capítulo, você encontrará os procedimentos para usar o Console do VirusScan a fim de configurar e personalizar a varredura planejada.

Usando o Console do VirusScan

Use o Console do VirusScan (Figura 5-1) para configurar uma varredura planejada. Inicie o Console do VirusScan clicando duas vezes no seu ícone no grupo de programas do VirusScan ou escolhendo **Console do McAfee VirusScan** no menu Ferramentas do VirusScan.

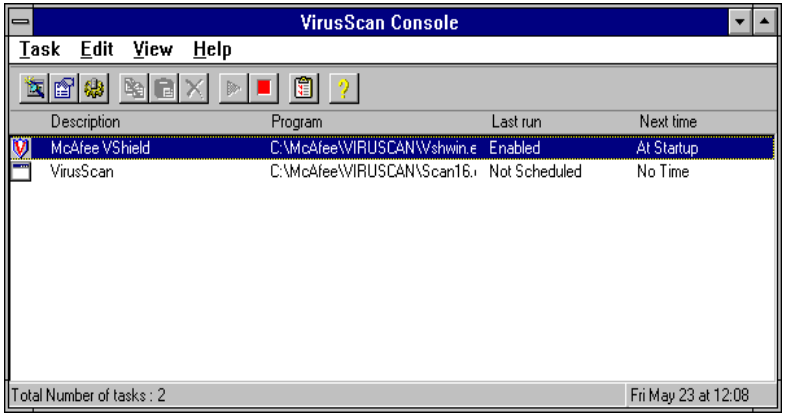

Figura 5-1. Console do VirusScan

Para exibir as propriedades da tarefa, clique duas vezes no seu nome ou clique com o botão direito do mouse na tarefa escolhida e selecione **Propriedades**. Aparece a janela Propriedades da tarefa (Figura 5-2 na página 42), mostrando a página Programa.

Criando uma tarefa de varredura

O Console do VirusScan usa as tarefas de varredura para executar e controlar as varreduras planejadas. Você pode configurar e planejar cada uma das tarefas separadamente, usando as páginas com guias na janela Propriedades da tarefa.

Selecionando o programa a ser executado

Siga estas etapas para selecionar o programa que executará uma nova tarefa:

1. No Console do VirusScan, escolha **Nova tarefa** no menu Tarefa ou clique com o botão direito do mouse na lista de tarefas e escolha **Nova tarefa**. Aparece a janela Propriedades da tarefa (Figura 5-2), mostrando a página Programa.

Figura 5-2. Janela Propriedades da tarefa (página Programa)

2. A localização padrão do arquivo de programa do VirusScan (**C:\Neta\Viruscan\SCAN16.EXE**) aparece na caixa de texto Programa, automaticamente. É possível digitar outra localização na caixa de texto ou procurar outro local.

3. Se você quiser usar o Console do VirusScan para planejar outro programa, digite o caminho correspondente na caixa de texto Programa.

NOTA: Utilize a caixa de texto Parâmetro para digitar um parâmetro de programa. Por exemplo, se estiver planejando usar o Notepad.exe, poderá digitar o nome de um arquivo de texto (por ex., WHATSNEW.TXT) para ser aberto quando o programa for executado.

4. Digite o nome da tarefa na caixa de texto Descrição.
5. Se quiser, clique em **Configurar senha** para definir uma senha para a tarefa. A caixa de diálogo mostrada pedirá que você digite e confirme a senha.
6. Configure as opções de varredura para a tarefa. Para fazer isso, veja "Configurando uma tarefa de varredura" na página 46.
7. Clique em **Executar agora**, se você quiser que a tarefa seja executada imediatamente.
8. Clique em uma das opções seguintes:
   - **OK** salva as alterações e retorna ao Console do VirusScan.
   - **Cancelar** ignora as alterações e retorna ao Console do VirusScan.
   - **Aplicar** efetua as alterações. Em seguida, outra página pode ser escolhida.

Configurando o planejamento da tarefa

Siga estas etapas para configurar o planejamento de uma tarefa de varredura:

1. Selecione a página Planejamento (Figura 5-3 na página 44). (A aparência da janela varia ligeiramente segundo as opções selecionadas.)

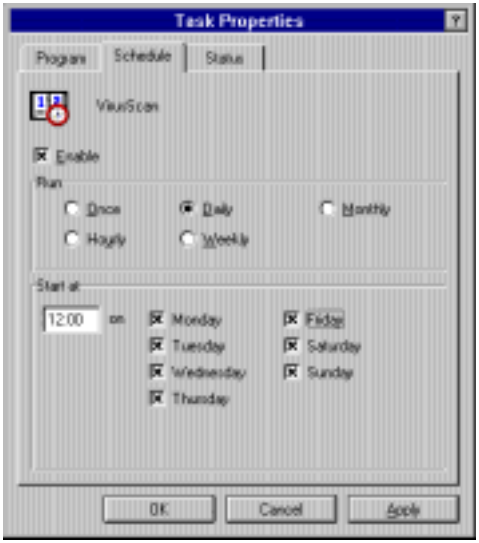

Figura 5-3. Janela Propriedades da tarefa (página Planejamento)

2. Selecione ou cancele a seleção **Ativar** para habilitar ou desativar a tarefa.

NOTA: Se a tarefa não estiver ativada, não será executada de acordo com o planejamento.

---

3. Especifique a freqüência da varredura:

   – Se você selecionar **Uma vez**, também determine a hora e a data da tarefa.

   – A escolha **Diariamente**, requer a especificação do(s) dia(s) da semana e da hora na qual a tarefa deverá ser executada.

   – Caso seja selecionada a opção **Mensalmente**, determine também o mês e a hora na qual a tarefa deve ser executada.

   – Se você escolher **A cada hora**, também selecione o número de minutos após cada hora em que a tarefa deve ser executada.

   – Se for selecionada a opção **Semanalmente**, também especifique o(s) dia(s) e a hora nos quais a tarefa deve ser executada.

NOTA: A hora deve ser digitada no formato de 24 horas (por ex., 20:27, e não 8:27 da noite) em todas as opções, exceto **A cada hora**.

---

4. Clique em uma das opções seguintes:
   - **OK** salva as alterações e retorna ao Console do VirusScan.
   - **Cancelar** ignora as alterações e retorna ao Console do VirusScan.
   - **Aplicar** insere as alterações. Em seguida, você poderá selecionar outra página.

Exibindo as propriedades da tarefa

1. Selecione a página Status (Figura 5-4) para exibir as estatísticas da tarefa atual.

Figura 5-4. Janela Propriedades da tarefa (página Status)

2. Clique em **OK** para sair da janela Propriedades da Tarefa e retornar o Console do VirusScan.

Copiando, colando ou excluindo uma tarefa de varredura

As tarefas podem ser copiadas ou coladas na lista de tarefas do Console do VirusScan. Esses procedimentos tornam rápida e fácil a criação de diversas tarefas semelhantes com configurações similares.

- Para copiar uma tarefa, escolha **Copiar** no menu Editar ou clique com o botão direito do mouse na tarefa selecionada e escolha **Copiar**.

- Para colar uma tarefa, selecione **Colar** no menu Editar ou clique com o botão direito do mouse na lista de tarefas e escolha **Colar**.
- Para excluir uma tarefa, selecione-a e pressione **EXCLUIR**.

Configurando uma tarefa de varredura

Para configurar onde e o quê o VirusScan irá examinar, clique em **Configurar** na página Programa da janela Propriedades da tarefa. Aparece a janela de Configuração, mostrando a página Detecção (Figura 5-5).

Figura 5-5. Janela de Configuração (página Detecção)

A janela de Configuração contém cinco páginas com guias. Para mover-se de uma para outra, clique na página escolhida, na parte superior da janela. As seções abaixo descrevem cada página em detalhe.

Usando a página Detecção

Use a página Detecção para especificar as unidades de disco, arquivos e pastas que o VirusScan deverá examinar. Siga estas etapas para configurar as opções de detecção para a varredura:

1. Adicione um ou mais itens à lista de varreduras. Para adicionar um item, selecione-o na lista Selecionar item para examinar.
   - **Meu computador** examina todas as unidades fixas, removíveis e de rede conectadas ao seu computador.

- **Todas as unidades removíveis** examina todas as unidades locais removíveis, como disquetes e CD-ROMs.
- **Todos os discos fixos** examina todos os discos rígidos locais.
- **Todas as unidades de rede** examina todas as unidades de rede mapeadas.

NOTA: Todos os diretórios e subdiretórios na localização selecionada serão examinados.

---

2. Adicione uma unidade de disco, arquivo ou pasta. Clique em **Selecione uma unidade ou pasta para examinar** e especifique o caminho do item a ser examinado.

NOTA: Clique em **Procurar** para navegar até o arquivo, a unidade de disco ou pasta.

---

3. Clique em **OK**. Os itens selecionados aparecerão na lista de Seleções.
4. Para remover um item da lista dos locais a serem examinados, selecione-o e clique em **Remover**.
5. Selecione os tipos de arquivos que o VirusScan irá examinar para buscar vírus.
   - **Todos os arquivos** examina todos os arquivos, de qualquer tipo. Esta opção resulta em uma varredura mais completa, porém mais lenta.
   - **Somente arquivos de programas** examina apenas os arquivos com determinadas extensões. Para editar as extensões incluídas nessa lista, clique em **Extensões**.

     NOTA: As extensões padrão são .EXE, .COM, .DO? e .XL? (o ponto de interrogação representa um coringa). Essa lista examina os arquivos de documentos e modelos do Word e Excel (.DOC, .DOT, .XLS e .XLT), bem como os arquivos de programas.

   - **Arquivos compactados** examina arquivos compactados com PKLITE ou LZEXE.
6. Selecione **Examinar a memória**, se você quiser examinar a memória do seu computador em busca de vírus.

7. Selecione **Iniciar automaticamnete** para que a tarefa seja iniciada automaticamente no horário planejado.

NOTA: Se a opção **Iniciar automaticamente** não for selecionada, o VirusScan será aberto no horário especificado, mas não concluirá a tarefa até que você clique em **Examinar agora**.

---

8. Selecione **Examinar setores de inicialização** para examinar o(s) setor(es) de inicialização da(s) unidade(s) especificada(s) nessa tarefa.

9. Se você quiser, clique em **Heurística de macro** para definir a varredura usada pelo VirusScan para limpar macros que possam conter vírus nos documentos do Microsoft Word e Excel. Aparece a caixa de diálogo Configurações da varredura heurística (Figura 5-6).

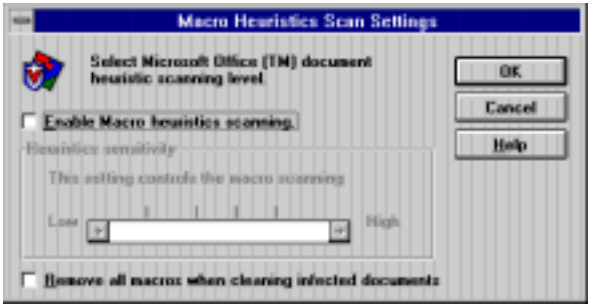

Figura 5-6. Caixa de diálogo Configurações da varredura heurística

a. Ativa ou desativa a varredura heurística de macro. O padrão é ativada.

b. Use o botão deslizante para definir a precisão da varredura.

c. Decida se o VirusScan removerá todas as macros ao limpar documentos infectados. Como padrão, o VirusScan remove todas as macros.

NOTA: Se o botão deslizante for movido para a posição Alta *e* for escolhida a opção Remover todas as macros ao limpar documentos infectados, o VirusScan removerá todas as macros de qualquer documento do Word ou Excel que for examinado — não apenas as macros semelhantes a vírus.

---

d. Clique em **OK**.

10. Faça o seguinte:
    - Clique em **Aplicar** para salvar as alterações.
    - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
    - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
    - Veja "Usando a página Segurança" na página 56 se quiser bloquear e proteger por senha as alterações.

Usando a página Ação

Use a página Ação para informar ao VirusScan o que fazer ao encontrar um vírus.

Siga estas etapas para configurar as opções de ação para uma varredura:

1. Selecione a página Ação. Aparece a janela de Configuração, mostrando a página Ação (Figura 5-7).

Figura 5-7. Janela de Configuração (página Ação)

2. Clique na seta ao lado da caixa de listagem, em seguida, escolha uma ação:

   - **Solicitar ação** faz o VirusScan perguntar o que deve fazer com cada vírus encontrado. Use esta ação se o computador estará supervisionado durante a varredura.

     Escolha as ações disponíveis para o VirusScan marcando as caixas de seleção em Ações possíveis.

   - **Mover arquivos infectados para um diretório** desloca automaticamente todos os arquivos infectados para um diretório de quarentena.

     Você deve informar ao VirusScan para onde os arquivos devem ser movidos. O padrão é **\infectado**. A menos que você especifique o caminho completo (por ex., **C:\meusdocumentos\infectado**), o VirusScan criará o diretório no nível raiz da unidade de disco, onde o vírus foi encontrado (por ex., **C:\infectado**).

   - **Limpar arquivos infectados** limpa automaticamente os vírus dos arquivos infectados.

   - **Excluir arquivos infectados** elimina automaticamente os arquivos infectados.

     NOTA: Os arquivos infectados são removidos permanentemente do seu sistema. Os arquivos excluídos devem ser restaurados a partir de cópias de backup.

   - **Continuar a varredura** faz com que o VirusScan prossiga com a varredura sem atuar sobre os arquivos infectados que encontrar.

3. Faça o seguinte:

   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja “Usando a página Segurança” na página 56, se quiser bloquear e proteger por senha as alterações.

Usando a página Alerta

Use a página Alerta para informar ao VirusScan como notificá-lo e a outras pessoas quando um vírus for encontrado. Siga estas etapas para configurar as opções de alerta para a varredura:

1. Selecione a página Alerta. Aparece a janela de Configuração, mostrando a página Alerta (Figura 5-8).

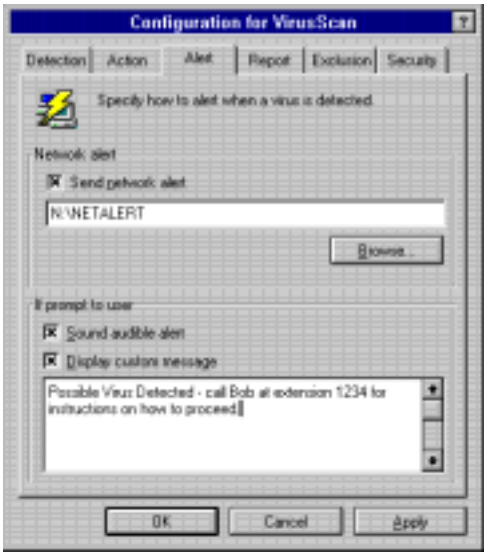

Figura 5-8. Janela de Configuração (página Alerta)

2. Se você quiser que o VirusScan envie um alerta de rede para um servidor que execute o NetShield, selecione**Enviar alerta de rede** e digite o caminho do arquivo de alerta.

NOTA: Esse caminho deve ser o de uma pasta que contém o arquivo de Alerta Centralizado, CENTALERT.TXT. Para obter mais informações sobre o Alerta Centralizado, veja a documentação do NetShield.

---

3. Se foi selecionada a opção **Solicitar ação** na página Ação, marque as caixas adequadas para que o VirusScan emita um alerta audível e/ou exiba uma mensagem personalizada. Você pode editar essa mensagem digitando um novo texto na caixa.

4. Faça o seguinte:
   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja "Usando a página Segurança" na página 56, se quiser bloquear e proteger por senha as alterações.

Usando a página Relatório

Use a página Relatório para especificar se o VirusScan registrará as suas ações e quais informações serão incluídas no registro. Siga estas etapas para configurar as opções de relatório para uma varredura:

1. Selecione a página Relatório. Aparece a janela de Configuração, mostrando a página Relatório (Figura 5-9).

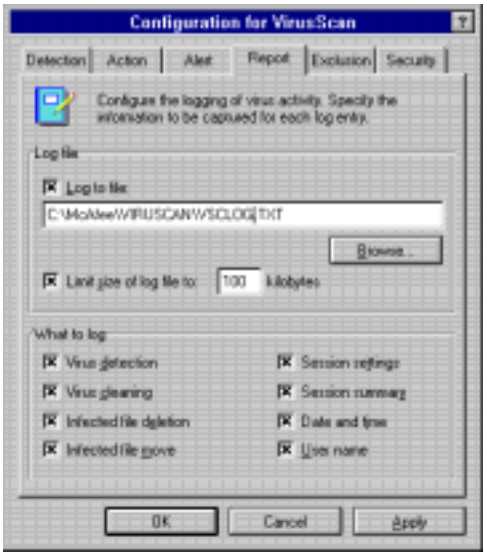

Figura 5-9. Janela de Configuração (página Relatório)

2. Para ativar o registro de uma atividade de varredura, selecione **Registrar no arquivo** e digite um caminho para um arquivo de texto.

   O caminho padrão é **C:\neta\virusscan\VSCLOG.TXT**. Esse arquivo é de texto simples e pode ser exibido em qualquer editor de texto, como o Bloco de Notas, bem como escolhendo **Exibir registro de atividades** no menu Arquivo.

3. Se você quiser limitar o tamanho do arquivo de registro, selecione **Limitar tamanho do arquivo de registro** e digite o tamanho máximo.

4. Marque as caixas de seleção mostradas para especificar quais informações devem ser incluídas no arquivo de registro. As opções disponíveis são:

   - Detecção de vírus
   - Limpeza de vírus
   - Eliminação do arquivo infectado
   - Movimentação do arquivo infectado
   - Configurações da sessão
   - Resumo da sessão
   - Data e hora
   - Nome do usuário.

5. Faça o seguinte:

   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja “Usando a página Segurança” na página 56, se quiser bloquear e proteger por senha as alterações.

Usando a página Exclusão

Use a página Exclusão (Figura 5-10) para informar ao VirusScan quais arquivos, pastas ou unidades devem ser excluídas durante a varredura.

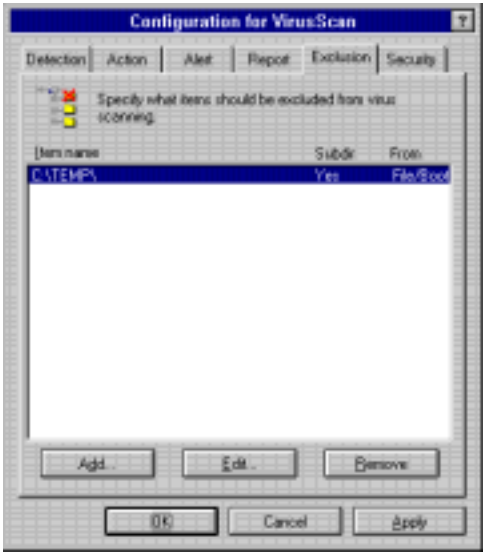

Figura 5-10. Janela de Configuração (página Exclusão)

Adicionando um item à lista de exclusão

Para adicionar um item na lista de exclusão, siga estas etapas:

1. Na página Exclusão, clique em **Adicionar**. Aparece a caixa de diálogo Excluir item (Figura 5-11).

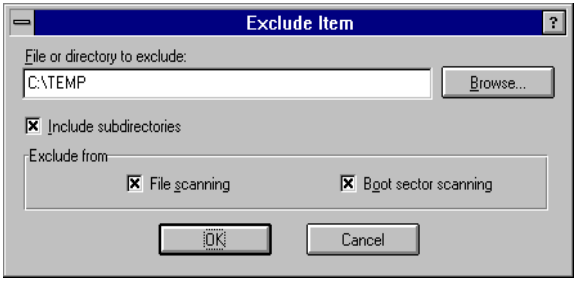

Figura 5-11. Caixa de diálogo Excluir item

2. Digite o caminho do item a ser excluído ou clique em **Procurar** para navegar até o item. Você pode excluir um arquivo, uma pasta ou um disco inteiro.
3. Selecione **Incluir subpastas** para que o VirusScan não examine as subpastas do item excluído da varredura.
4. Indique se deseja que a pasta seja excluída da varredura de arquivo ou do setor de inicialização, marcando a(s) caixa(s) adequada(s).
5. Clique em **OK**.
6. Selecione de quais tipos de varreduras você deseja excluir esse item:
   - Para excluir o item da varredura de arquivo, escolha **Varredura de arquivo**
   - Para excluir o item da varredura do setor de inicialização, escolha **Varredura de setor de inicialização**.
7. Faça o seguinte:
   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja "Usando a página Segurança" na página 56 se quiser bloquear e proteger por senha as alterações.

Removendo um item da lista de exclusão

Para remover um item da lista, siga estas etapas:

1. Na página Exclusão, selecione o item a ser removido, em seguida, clique em **Remover**.
2. Faça o seguinte:
   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja "Usando a página Segurança" na página 56, se quiser bloquear e proteger por senha as alterações.

Editando um item na lista de exclusão

Para editar um item existente na lista de exclusão, siga estas etapas:

1. Na página Exclusão, selecione o item a ser editado, em seguida, clique em **Editar**.
2. Aparece a caixa de diálogo Excluir item (Figura 5-11 na página 54). Faça as alterações necessárias, em seguida, clique em OK.
3. Faça o seguinte:
   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.
   - Veja “Usando a página Segurança” na página 56, se quiser bloquear e proteger por senha as alterações.

Usando a página Segurança

Use a página Segurança para proteger por senha as configurações do VirusScan e impedir que alterações não intencionais sejam feitas. Siga estas etapas para configurar as opções de segurança para a varredura:

1. Selecione a página Segurança (Figura 5-12 na página 57).

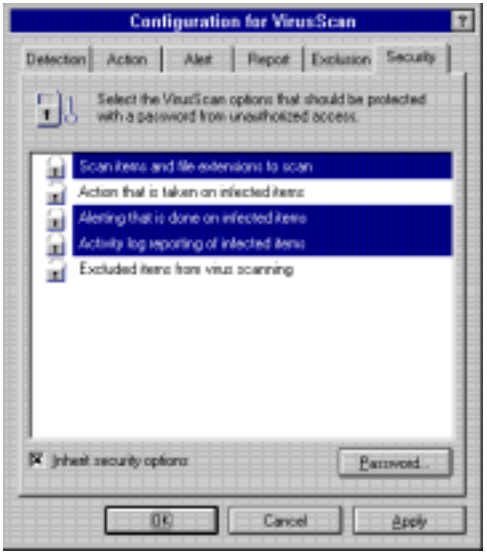

Figura 5-12. Janela de Configuração (página Segurança)

2. Selecione as configurações do VirusScan que serão protegidas por senha:
   - **Itens de varredura e extensões de arquivo a serem examinadas**
   - **Ação tomada para os itens infetados**
   - **Alerta para os itens infectados**
   - **Relatório do arquivo de atividades sobre os itens infectados**
   - **Itens excluídos da varredura**.

NOTA: As configurações protegidas por senha são colocadas em destaque na lista e o cadeado, à sua esquerda estará fechado.

---

3. Selecione **Herdar opções de segurança**, se você quiser que as opções selecionadas sejam incluídas, como padrão, nas cópias dessa tarefa.

NOTA: Se a opção **Herdar opções de segurança** for selecionada na tarefa principal do VirusScan, as opções de segurança para essa tarefa serão herdadas por **todas** as novas tarefas, bem como as cópias da tarefa principal do VirusScan.

---

4. Se ainda não tiver sido criada uma senha, faça-o clicando em **Senha**. Você será solicitado a digitar e confirmar a sua senha.

   Se você já tiver uma senha, poderá alterá-la agora ou quando quiser, clicando em **Senha**. Digite e confirme a sua nova senha.

5. Faça o seguinte:

   - Clique em **Aplicar** para salvar as alterações.
   - Clique em **OK** para salvar as alterações e retornar ao Console do VirusScan.
   - Clique em **Cancelar** para retornar ao Console do VirusScan sem salvar as alterações.

Removendo um vírus 6

Se há suspeita de vírus

Se houver um vírus no seu sistema antes da instalação do VirusScan para Windows 3.1*x*— ou haja suspeita de infecção — siga este procedimento para criar um ambiente desinfectado.

1. Desligue o computador.

   NOTA: Não o reinicie usando o botão Reset ou CTRL+ALT+DELETE; se isso ocorrer, alguns vírus podem ficar intactos.

   ---

2. Faça um Disco de Emergência. Veja "Criando um Disco de Emergência" na página 72 para obter mais detalhes.
3. Insira-o na unidade A: e ligue o computador.
4. Faça o seguinte:
   - Se for possível criar o Disco de Emergência com o utilitário de criação automática, basta seguir as instruções na tela.
   - Se for utilizado um disquete de inicialização limpo, criado manualmente, digite:

     ```
     scan /ADL /ALL /CLEAN
     ```

     no prompt de comando. Esse procedimento inicia a versão de linha de comando do VirusScan. O andamento da operação será exibido na tela.

   NOTA: Para obter informações detalhadas sobre as opções de linha de comando do VirusScan, veja Apêndice D, "Referência".

Se os vírus forem removidos

Se o VirusScan remover com sucesso todos os vírus, desligue o seu computador e remova o disquete. Reinicie o computador e continue a trabalhar. Se você estava instalando o VirusScan, inicie o procedimento de instalação descrito no Capítulo 2, “Instalando o VirusScan”.

Para localizar e eliminar a origem da infecção, examine todos os seus disquetes imediatamente antes da instalação.

Se os vírus não forem removidos

Se o VirusScan não puder remover um vírus, enviará uma das seguintes mensagens:

- O vírus não pôde ser removido.
- Não há removedor disponível para o vírus atualmente.

Se você receber uma dessas mensagens, conulte os documentos relativos à remoção manual de vírus no site da Web da Network Associates. Para obter informações sobre contato, veja “Como contactar a Network Associates” na página xvii.

Se o VirusScan detectar um vírus

Os vírus atacam o computador através da infecção de arquivos — normalmente, dos programas executáveis ou arquivos de documentos. Com freqüência, esses arquivos são danificados durante a infecção. O VirusScan pode remover seguramente muitos vírus de arquivos infectados. Contudo, alguns vírus são projetados para danificar os seus arquivos a ponto de ficarem irrecuperáveis. Esses arquivos, chamados de arquivos “danificados”, podem ser movidos pelo VirusScan para um diretório de quarentena ou excluídos, para evitar que outro vírus infeccione o seu sistema.

Removendo um vírus encontrado em um arquivo

Se o VirusScan detectar um vírus em um arquivo, realizará a ação que você especificou durante a configuração. Veja “Configurando as ações do VShield” na página 14.

Removendo um vírus encontrado na memória

Se o VirusScan detectar um vírus no seu sistema, limpe-o imediatamente para impedir que o vírus se espalhe no PC ou na rede. Remova os vírus dos arquivos, se você souber ou suspeitar que estão infectados.

Caso um vírus esteja residindo na memória ou tenha infectado o Registro de inicialização principal (MBR) ou o setor de inicialização, desligue o computador, reinicie-o com um Disco de Emergência. Em seguida, remova o vírus usando a versão de linha de comando do VirusScan. Para obter mais informações, veja “Se há suspeita de vírus” na página 59 e o Apêndice C, “Instalações compartilhadas”. Certifique-se de usar somente a varredura de linha de comando para limpar o seu sistema, se um vírus for detectado na memória.

Compreendendo os alarmes falsos

Um alarme falso é um relato de um vírus em um arquivo ou na memória, quando não há nenhum. Os alarmes falsos podem ocorrer se você tiver mais de uma marca de software de detecção de vírus em seu computador, porque alguns programas antivírus armazenam as seqüências de caracteres de assinatura desprotegidas na memória. Como resultado disso, o VirusScan pode “detectá-los” falsamente como vírus. O BIOS do seu sistema, o uso de códigos de validação e outros fatores também podem produzir alarmes falsos.

Suponha sempre que qualquer vírus encontrado pelo VirusScan é real e perigoso, e realize as etapas necessárias para removê-lo do sistema. Se, contudo, você tiver razões para acreditar que o VirusScan esteja gerando um alarme falso (por exemplo, o programa detectou um vírus em um único arquivo que você usa há anos sem apresentar problemas), consulte a lista de origens potenciais abaixo:

- O VirusScan pode gerar um alarme falso se mais de um programa antivírus estiver em execução. Configure o seu computador para que execute um programa antivírus de cada vez. Retire as linhas do arquivo AUTOEXEC.BAT que se refiram a outros programas antivírus. Desligue o computador, aguarde alguns segundos e ligue-o novamente para certificar-se de que todo o código relativo aos outros programas foi removido da memória.
- Alguns chips de BIOS incluem um recurso antivírus que pode originar alarmes falsos. Consulte o manual de referência do seu computador para obter mais detalhes.

- Se você configurar códigos de validação / recuperação, as varreduras subseqüentes poderão detectar alterações nos arquivos validados. Isto pode acionar alarmes falsos se os arquivos executáveis forem automodificadores ou autoverificadores. Ao usar os códigos de validação, especifique na lista de exceções que esses arquivos devem ser excluídos da varredura.
- Alguns PCs da Hewlett-Packard e Zenith mais antigos modificam o setor de inicialização sempre que o sistema é inicializado. O VirusScan pode detectar essas modificações como uma possível infecção, mesmo que não haja vírus. Consulte o manual de referência do seu computador para determinar se o código de inicialização do PC é automodificador. Para solucionar esse problema, salve as informações de validação / recuperação nos arquivos executáveis; esse método não salva as informações sobre o setor de inicialização ou o Registro de inicialização principal.
- O VirusScan pode relatar vírus no setor de inicialização ou no Registro de inicialização principal de certos disquetes protegidos contra cópia.

Network Associates Serviços de suporte

A

A escolha do software antivírus e de segurança da Network Associates ajuda a assegurar que a tecnologia de informação crítica na qual você baseia-se funciona perfeitamente e com eficiência. Os benefícios do plano de suporte da Network Associates estende a proteção obtida com o seu software dando-lhe as instruções necessárias para instalar, monitorar, fazer a manutenção e atualizar a versão do sistema com a tecnologia mais recente da Network Associates. Com o plano de suporte projetado para atender as suas necessidades, você pode manter o sistema ou a rede funcionando de forma confiável em seu ambiente de computação por muitos meses ou anos.

Os planos de suporte da Network Associates são oferecidos em duas categorias. Se você for um cliente corporativo, poderá escolher entre três níveis de suporte prolongado no programa PrimeSupport da Network Associates. Se tiver adquirido uma versão para o varejo de um produto da Network Associates, poderá escolher um plano dirigido às suas necessidades no plano Suporte Pessoal.

Opções do PrimeSupport para clientes corporativos

O programa PrimeSupport da Network Associates oferece as opções Básico, Estendido ou Permanente. Cada opção apresenta diversos recursos que fornecem suporte imediato e econômico dirigido para atender as suas necessidades.

Opção PrimeSupport Básico

A opção PrimeSupport Básico lhe oferece acesso telefônico aos membros experientes da equipe de suporte técnico da Network Associates para obter assistência ao produto. Se você adquiriu o software da Network Associates com uma licença de assinatura, recebeu a opção PrimeSupport Básico como parte do pacote de dois anos a partir da data de compra. Se tiver adquirido o produto da Network Associates com uma licença permanente, poderá renovar o seu plano de PrimeSupport Básico após o pagamento de uma taxa anual.

A opção PrimeSupport Básico inclui estes recursos:

- Acesso telefônico ao suporte técnico de segunda a sexta, das 8:00 às 20:00, Horário Central dos EUA.

- Acesso 24 horas irrestrito às informações do suporte técnico, através do site da Web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão do produto, através do site da Web da Network Associates.

Opção PrimeSupport Estendido

O PrimeSupport Estendido lhe oferece suporte personalizado e dinâmico de um engenheiro de suporte técnico específico. Estará à sua disposição um profissional de suporte que está familiarizado com a distribuição e histórico de suporte do seu produto da Network Associates, e que entrará em contato em intervalos que você determina para verificar se você sabe usar e fazer a manutenção dos produtos da Network Associates. Telefonando com antecedência, o representante do PrimeSupport Estendido poderá ajudá-lo a evitar problemas antes que ocorram. Se, contudo, houver um caso de emergência, o PrimeSupport Estendido estabelecerá um prazo de resposta para assegurar que a ajuda está a caminho. O PrimeSupport Estendido pode ser adquirido por um ano a partir da compra de um produto da Network Associates com uma licença de assinatura ou permanente.

O PrimeSupport Estendido inclui estes recursos:

- Acesso a um engenheiro de suporte específico.
- Contatos de suporte dinâmico através de telefone ou correio eletrônico com o seu engenheiro de suporte específico, a intervalos determinados por você.
- Prazos de resposta: o seu engenheiro de suporte responderá em uma hora ao pager, em quatro horas ao correio de voz e em 12 horas ao correio eletrônico.
- Acesso telefônico ao suporte técnico de segunda a sexta, das 7:00 às 19:00. Hora Central dos EUA.
- Acesso 24 horas irrestrito às informações do suporte técnico, através do site da Web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão através do site da Web da Network Associates.
- Possibilidade de designar até cinco pessoas em sua organização como contatos do cliente.

PrimeSupport Permanente

O PrimeSupport Permanente lhe oferece suporte dinâmico e personalizado, 24 horas, para os produtos da Network Associates distribuídos nos sistemas de informação sobre negócios mais críticos. O PrimeSupport Permanente coloca à sua disposição os recursos do PrimeSupport Estendido durante 24 horas, sete dias na semana, com o menor tempo de resposta. Você pode adquirir o PrimeSupport Permanente durante um período anual ao comprar um produto da Network Associates com uma licença de assinatura ou permanente.

O PrimeSupport Permanente inclui estes recursos:

- Acesso a um engenheiro de suporte específico.
- Contatos de suporte dinâmico através de telefone ou correio eletrônico com o seu engenheiro de suporte específico, a intervalos determinados por você.
- Prazos de resposta: o seu engenheiro de suporte responderá em meia hora ao pager, em uma hora ao correio de voz e em quatro horas ao correio eletrônico.
- Acesso telefônico ao suporte técnico 24 horas, sete dias na semana.
- Acesso 24 horas irrestrito às informações do suporte técnico, através do site da Web da Network Associates.
- Atualizações dos arquivos de dados e atualizações de versão através do site da Web da Network Associates.
- Possibilidade de designar até dez pessoas em sua organização como contatos do cliente.

Tabela A-1. PrimeSupport Imediato

Recurso	Básico	Estendido	Permanente
Suporte técnico pelo telefone	De segunda a sexta de 8:00 às 20:00.	De segunda a sexta de 7:00 às 19:00.	de 7:00 às 19:00. 24 horas, 7 dias na semana
Suporte técnico no site da Web	Sim	Sim	Sim
Atualizações do software	Sim	Sim	Sim
Engenheiro de suporte específico	—	Sim	Sim
Contato de suporte dinâmico	—	Sim	Sim

Tabela A-1. PrimeSupport Imediato

Recurso	Básico	Estendido	Permanente
Contatos de suporte designados	—	5	10
Prazo de resposta	—	Pager: 1 hora Correio de voz: 4 horas Correio eletrônico: 12 horas	Pager: 30 min. Correio de voz: 1 hora Correio eletrônico: 4 horas

Pedindo o PrimeSupport

Para pedir o PrimeSupport Básico, Estendido ou Permanente para os produtos da Network Associates: Entre em contato com o seu representante de vendas, ou

- Entre em contato com o seu representante de vendas, ou
- Ligue para os Serviços de Suporte da Network Associates no telefone 1-800-988-5737 ou 00-1-650-473-2000, de segunda a sexta , de 6:00 às 17:00. Hora do Pacífico.

O programa PrimeSupport descrito neste guia está disponível somente na América do Norte. Para conhecer as opções do PrimeSupport disponíveis fora da América do Norte, entre em contato com o escritório de vendas regional. As informações sobre contato aparecem no incío deste guia.

Serviços de suporte para clientes do varejo

Se você adquirir o seu produto da Network Associates através de um varejista local ou do site da Web da Network Associates, também receberá alguns serviços de suporte como parte de sua compra. Este nível específico de suporte incluído depende do produto adquirido. Os exemplos dos serviços recebidos incluem:

- Arquivo (.DAT) de dados gratuito, atualizações durante a vida de seu produto através do site da Web da Network Associates, o recurso AutoUpdate do produto ou o serviço SecureCast. Você também pode atualizar os seus arquivos de dados usando um navegador da Web para visitar o site:

  http://www.nai.com/download/updates/updates.asp

- Atualizações de versão do programa (arquivo executável) gratuito durante um ano através do site da Web da Network Associates, o recurso AutoUpdate do produto ou o serviço SecureCast. Se você adquirir uma versão especial do produto da Network Associates, receberá atualizações de versão do produto gratuitas durante dois anos. A atualização de versão do software também pode ser feita usando o seu navegador da Web para visitar o site:

  http://www.nai.com/download/upgrades/upgrades.asp

- Acesso gratuito 24 horas, sete dias na semana a suporte online ou eletrônico via sistema de voz ou fax, ou site da Web da Network Associates e através de outros serviços eletrônicos, como America Online e CompuServe.

  Para entrar em contato com os serviços eletrônicos da Network Associates escolha uma destas opções:

  – Sistema de voz e fax automático: (408) 988-3034

  – Site da Web da Network Associates: **http://support.nai.com**

  – CompuServe: GO NAI

  – America Online: palavra-chave MCAFEE

- Noventa dias de suporte de cortesia fornecido por um técnico de suporte da Network Associates durante horário comercial, de segunda a sexta, das 8:00 às 18:00. Hora Central dos EUA.

  Após expirar o período de suporte de cortesia, você poderá beneficiar-se das várias opções de suporte pessoal dirigidas para atender às suas necessidades. Entre em contato com a Assistência ao Cliente da Network Associates através do telefone 00 1 (972) 278-6100 para conhecer as opções disponíveis, ou visite o site da Web da Network Associates em:

  http://www.nai.com/services/support/support.asp

Treinamento e Consultoria da Network Associates

A Network Associates fornece consultoria profissional de alto nível e treinamento completo que podem ajudá-lo a maximimizar a segurança e o desempenho da sua rede de investimentos através do programa Total Service Solutions da Network Associates.

Serviços de consultoria profissional

Os Serviços de consultoria profissional da Network Associates estão prontos para dar assistência em todos os estágios do desenvolvimento da sua rede, do planejamento e desenho à implementação, com gerenciamento contínuo. Os consultores da Network Associates oferecem recursos suplementares profissionais e perspectiva independente para resolver os seus problemas. Você obterá ajuda para integração dos produtos da Network Associates ao seu ambiente, bem como assistência para a solução de problemas ou ajuda para estabelecer as bases do desempenho de uma rede. Os consultores da Network Associates também desenvolvem e sugerem soluções personalizadas para ajudá-lo a atingir os objetivos de seus projetos — de implementações extensas e em larga escala à solução de pequenos problemas.

Serviços educacionais completos

Os Serviços educacionais completos da Network Associtates desenvolvem e aprimoram as habilidades de todos os profissionais de rede através de instruções práticas que podem ser utilizadas imediatamente em seu trabalho. O currículo da tecnologia Serviços educacionais completos é dirigida para o gerenciamento do desempenho e das falhas de rede, além de abranger a solução de problemas em todos os níveis. A Network Associates oferece também treinamento de produto modular para que você possa compreender os recursos e funcionalidade do seu novo software.

A inscrição para os cursos dos Serviços educacionais completos está aberta o ano inteiro nos centros educacionais da Network Associates, ou você poderá aprender nos cursos personalizados, implementados em seu local de trabalho. Todos os cursos seguem etapas educacionais em uma linha de aprendizado que o leva ao mais alto nível técnico. A Network Associates é membro fundador do consórcio Certified Network Expert (CNX).

Para obter mais informações sobre esses programas, entre em contato com o seu representante de vendas ou ligue para Total Service Solutions no telefone 00 1-800-395-3151.

Evitando a infecção por vírus B

Procedimentos importantes para manter um ambiente de sistema seguro

O VirusScan para Windows 3.1*x* é uma ferramenta eficiente para evitar, detectar e recuperar o sistema de uma infecção por vírus. Contudo, é mais efetivo quando faz parte de um programa completo de segurança de computação que inclui vários procedimentos como backups, proteção significativa por senha, treinamento do usuário e conscientização.

Para criar um ambiente de sistema seguro e minimizar as chances de infecção, a Network Associates recomenda que você execute as etapas abaixo:

- Siga os procedimentos de instalação descritos no Capítulo 2, "Instalando o VirusScan". Se você suspeitar que há uma infecção por vírus, execute as etapas para limpar o seu sistema, antes de instalar o VirusScan. Para saber como fazê-lo, veja "Se há suspeita de vírus" na página 59.
- Configure o arquivo AUTOEXEC.BAT para que carregue o VShield automaticamente na inicialização.

NOTA: O seu arquivo AUTOEXEC.BAT é modificado se os procedimentos de instalação recomendados forem seguidos.

- Crie um disco de instalação que contenha a versão de linha de comando do VirusScan, seguindo o procedimento descrito em "Criando um Disco de Emergência" na página 72. Certifique-se de que o disquete esteja protegido contra garvação para que não possa ser infectado.
- Faça backups freqüentes dos arquivos importantes. Mesmo com o VirusScan, alguns vírus (bem como fogo, roubo ou vandalismo) podem tornar um disco, sem um backup recente, irrecuperável.

Embora não seja o objetivo deste manual descrever um programa de segurança completo, seguir as etapas descritas neste apêndice o ajudarão a compreender com clareza o que são os vírus, como afetam o sistema e o que pode ser feito para evitar uma infecção.

Detectando vírus novos e desconhecidos

Há duas maneiras de tratar os vírus novos e desconhecidos que podem afetar o seu sistema:

- Atualizar os arquivos de dados do VirusScan
- Atualizar os arquivos de programa do VirusScan.

O VirusScan usa os arquivos (.DAT) de dados para detectar vírus. A atualização regular desses arquivos pode proteger o seu sistema contra as ameaças de vírus mais recentes. A Network Associates os atualiza mensalmente para fornecer maior proteção contra novos vírus. Com menos freqüência, a Network Associates altera o programa VirusScan para aumentar a proteção e adicionar recursos. Quando isso acontece, você deve atualizar a versão da sua instalação para a mais recente do VirusScan.

Atualizando os arquivos de dados do VirusScan

Para oferecer a melhor proteção contra vírus possível, a Network Associates atualiza continuamente os arquivos utilizados pelo VirusScan para detectar vírus. Após um determinado período de tempo, você recebe um aviso para atualizar o banco de dados de definições de vírus. A Network Associates recomenda que esses arquivos sejam atualizados regularmente para obter máxima proteção.

O que é um arquivo de dados?

Os arquivos CLEAN.DAT, NAMES.DAT e SCAN.DAT fornecem informações sobre vírus para o software VirusScan. Estes são os arquivos de dados aos quais nos referimos nesta seção.

Por que é necessário um novo arquivo de dados?

Novos vírus são descobertos a uma média de mais de 200 por mês. Com freqüência, esses novos vírus não são detectados quando são utilizados arquivos de dados mais antigos. Os arquivos de dados que acompanham a sua cópia do VirusScan podem não ser capazes de ajudar o programa a detectar um vírus descoberto meses após a aquisição do produto.

Os pesquisadores da Network Associates trabalham constantemente para atualizar os arquivos de dados a fim de acrescentar outras definições de vírus mais novos.

NOTA: A Network Associates oferece atualizações de arquivo de assinatura de vírus online durante a vida de seu produto. Contudo, não podemos garantir a compatibilidade inversa dos arquivos de assinatura de vírus para um software de versão anterior. Ao atualizar para a versão mais recente do VirusScan, você manterá o melhor nível de defesa contra ameaças de vírus.

Como aplicar o arquivo de dados

Para atualizar os seus arquivos de dados, siga as etapas abaixo.

1. Faça download do arquivo de dados (por exemplo, DAT-3004.ZIP) a partir de um dos serviços eletrônicos da Network Associates. Na maioria dos serviços, o arquivo de dados está localizado na área de antivírus.

   NOTA: O seu acesso a essas atualizações está restrito legalmente pelos termos de manutenção descritos no arquivo README.1ST, que acompanha o software, e detalhados no contrato de licença do software.

2. Copie o arquivo para um novo diretório.
3. O arquivo está no formato compactado. Descompacte o arquivo usando qualquer software de descompactação compatível com PKUNZIP. Se você não tiver este software, poderá obter por download o PKUNZIP (shareware) nos sites eletrônicos da Network Associates.
4. Localize os diretórios no disco rígido nos quais o software VirusScan está carregado atualmente (normalmente, em **C:\Neta\Viruscan)**. Este local varia dependendo da sua versão do software e se foi especificado um diretório diferente durante a instalação.
5. Copie os novos arquivos para esse(s) diretório(s), sobrepondo os arquivos de dados antigos.

   NOTA: Deve haver partes do software em mais de um diretório. Se isso ocorrer, coloque os arquivos atualizados em cada diretório.

6. O computador deve ser reiniciado para que o VirusScan reconheça e possa usar os arquivos atualizados.

Validando os arquivos de programa do VirusScan

Quando você fizer download de um arquivo a partir de uma BBS ou de outro serviço eletrônico da Network Associates, deverá verificar se o arquivo é autêntico, não foi alterado, nem está infectado. O software antivírus da Network Associates inclui um programa utilitário chamado Validação, que pode ser usado para assegurar que a sua versão do VirusScan é autêntica. Ao receber uma nova versão do VirusScan, execute o utilitário Validação em todos os arquivos de programa. Para obter mais detalhes sobre o programa Validação, veja o arquivo de texto README.1ST que acompanha o software.

Criando um Disco de Emergência

Se o sistema for infectado, você deve dispor de um Disco de Emergência. Esta seção descreve como criá-lo.

O seu sistema não deve estar infectado ao fazer um Disco de Emergência. Qualquer vírus residente no sistema pode ser transferido para esse disco e reinfectar o sistema.

Se houver suspeita de que o seu computador está infectado, procure outra máquina e examine-a. Caso esteja sem vírus, siga as etapas abaixo, que detalham como usar o utilitário de criação de Disco de Emergência, incluído no VirusScan.

NOTA: Se houver suspeita de que o computador está infectado mas não for possível encontrar outro computador com o VirusScan instalado, veja “Criando um disquete de inicialização limpo” na página 73, que ensina a criar manualmente um disco de inicialização limpo. Isto pode servir como um substituto para um Disco de Emergência até que você instale o VirusScan e possa criá-lo.

---

1. Insira um disquete em branco na unidade A:.
2. Execute o utilitário de criação de Disco de Emergência clicando duas vezes no ícone correspondente no grupo de programas do VirusScan.
3. Siga as instruções na tela. Se houver um problema na criação de um Disco de Emergência, certifique-se de que o disco inserido não esteja protegido contra gravação.
4. Quando o utilitário de criação de Disco de Emergência terminar sua execução, remova o disquete da unidade. Proteja o disquete contra gravação, etiquete e guarde-o em local seguro. Para obter mais informações, veja “Protegendo um disquete contra gravação” na página 74.

Criando um disquete de inicialização limpo

Se você estiver trabalhando em um computador que não tem o VirusScan, poderá criar um disquete de inicialização limpo. Esse disquete servirá como um substituto para um Disco de Emergência até que você possa instalar o VirusScan e usar o utilitário de criação de Disco de Emergência incluído.

Para criar um disquete de inicialização limpo, siga estas etapas a partir do prompt do DOS (você deve ir para o DOS ou abrir uma janela do DOS):

NOTA: Esse procedimento deve ser executado em um sistema livre de vírus.

---

1. Insira um disquete em branco na unidade A:.
2. Formate o disquete digitando o seguinte comando no prompt **C:\>**:

   ```
   format a: /s /u
   ```

3. Esse procedimento sobrepõe qualquer informação já existente no disquete.

   NOTA: Se você estiver usando o DOS 5.0 ou uma versão anterior, não digite /u. Se não souber ao certo qual é a sua versão, digite **ver** no prompt **C:\>** para obter informação sobre a versão.

   ---

4. Quando o sistema lhe pedir um rótulo para o volume, digite um nome adequado com onze caracteres, no máximo.
5. Altere o diretório VirusScan digitando o seguinte comando no prompt **C:\>**:

   ```
   cd \mcafee\viruscan
   ```

6. Copie a versão para DOS do VirusScan no disquete digitando os seguintes comandos no prompt **C:\mcafee\viruscan**:

   ```
   copy scan.exe a:
   copy scan.dat a:
   copy clean.dat a:
   copy names.dat a:
   ```

7. Volte para o diretório raiz digitando o seguinte comando no prompt **C:\mcafee\viruscan**:

   ```
   cd\
   ```

8. Copie no disquete os programas do DOS úteis digitando o seguinte comando no prompt C:\:

   ```
   copy c:\dos\chkdsk.* a:
   ```

9. Repita a última etapa para qualquer outro programa a ser adicionado no disquete. Abaixo, estão alguns programas que você possa querer:

   - debug.*
   - diskcopy.*
   - fdisk.*
   - format.*
   - label.*
   - mem.*
   - sys.*
   - unerase.*
   - xcopy.*

   NOTA: Se você utilizar um utilitário de compactação, certifique-se de que copiou os drivers necessários para ter acesso aos disquetes compactados no Disco de Emergência. Veja na documentação o utilitário de compactação para obter mais informações sobre esses drivers.

10. Etiquete o disquete e proteja-o contra gravação, em seguida, guarde-o em local seguro. Veja "Protegendo um disquete contra gravação" na página 74 para obter mais informações.

Protegendo um disquete contra gravação

Os disquetes são dispositivos práticos e portáteis para armazenar e recuperar dados de computador. Os disquetes são usados para salvar arquivos (gravar) e recuperá-los (ler). São também o veículo mais comum usado pelos vírus para invadir o sistema do seu computador.

Um modo de ajudá-lo a evitar infecção através de disquete é *protegê-lo contra gravação* tornando os dados somente para leitura. Se o seu sistema não estiver infectado por um vírus, o recurso de proteção contra gravação impedirá que os disquetes limpos sejam infectados, evitando a reinfecção após a limpeza do sistema.

NOTA: Qualquer disquete que não esteja protegido contra gravação deve ser examinado e limpo antes da proteção contra gravação.

Protegendo disquetes de 3,5” contra gravação

1. Coloque o disquete com a face para baixo com a proteção de metal deslizante à sua frente.

   Examine o orifício retangular na parte superior esquerda. Deve haver uma lingüeta quadrada de plástico que você pode deslizar para cima e para baixo nesta abertura.

2. Para proteger o disquete contra gravação, deslize a lingüeta de plástico para cima em direção à extremidade do disquete para que o orifício fique aberto.

Instalações compartilhadas C

Procedimento geral

1. Registre-se em uma conta como administrador de uma estação de trabalho compartilhada através do Windows 3.1*x*.
2. Realize o processo de instalação que inicia na página 5. Onde for necessário, altere o diretório adequado para uma instalação compartilhada.
3. Ao terminar a instalação, reinicie o computador na mesma conta de administrador.
4. Faça as modificações descritas na próxima seção.

Alterações nos arquivos

Arquivo Win.ini

Adicione a seguinte entrada na seção [VirusScan] do arquivo WIN.INI:

```
naiinipath=x:\test\folder
```

Essa entrada permite estabelecer um local alternativo para o arquivo AVCONSOL.INI.

Arquivo Autoexec.bat

Se você quiser colocar os DATs em uma pasta separada, deverá adicionar uma entrada como a seguinte no arquivo AUTOEXEC.BAT.

```
set mcafee.scan=x:\test\DATS
```

Essa entrada permite que o SCAN.EXE ou o SCANPM.EXE continue a funcionar da maneira especificada.

Arquivo Avconsol.ini

Novas entradas

Há duas novas entradas na seção [VirusScan Console] do arquivo AVCONSOL.INI.

- `RefreshRate=3` informa a configuração, em segundos, para a freqüência com que o AVCONSOL.EXE verifica as alterações no arquivo .INI. Esse valor pode ser definido entre 1 e 10 segundos.

  NOTA: O acesso à rede é reduzido significativamente, se for configurado um valor mais alto.

- `NewTaskPath=x:\new=vscfile` informa a localização padrão onde será armazenada uma nova tarefa criada no AVCONSOL.EXE.

Arquivos de configuração do VShield

O local do arquivo de configuração do VShield pode ser alterado através da edição da seção [Item-0] no AVCONSOL.INI. Na [Item-0], deve haver uma entrada chamada SzVshFile.

Adicione uma entrada semelhante em:

```
SzVshFile=x:\test\directory
```

Esse procedimento adiciona o recurso de busca no diretório onde você deseja que o arquivo de configuração do VShield resida.

NOTA: Se a entrada SzVshFile não for localizada, adicione-a em [Item-0].

Arquivos de configuração da Scan16

Se você quiser colocar os arquivos de configuração da tarefa Scan16 em um diretório separado, modifique a entrada SzVscFile em cada item do AVCONSOL.INI que indique uma entrada Scan16.

Limitações

Os tipos particulares de instalações compartilhadas impõem limitações às atualizações de status e de registro.

Atualizações de status

Se um usuário tiver acesso ao AVCONSOL.EXE com direito somente para leitura para o diretório no qual reside o arquivo de configuração, o status não será atualizado por qualquer função que a conta tente usar. Mesmo que a conta do usuário execute uma tarefa planejada, não haverá indicação de que isso ocorreu.

NOTA: Essa limitação não se aplica às contas de administradores.

Registro

Se os arquivos executáveis forem instalados em um diretório para o qual as contas dos usuários tenham apenas o acesso de leitura, os diretórios de registro devem permitir acesso de leitura e gravação para que o registro possa ser feito com precisão.

Caso os resultados do sistema, para todos os usuários, sejam registrados no mesmo arquivo, este deve ser configurado para o tamanho máximo.

Referência D

Opções da linha de comando do VirusScan

A seguinte tabela contém uma lista de todas as opções do VirusScan que podem ser utilizadas quando você estiver executando a varredura de linha de comando do DOS, SCAN.EXE. Para executar o VirusScan para Windows 3.1*x* na linha de comando, use primeiro o comando `cd`, a fim de ir para o diretório no qual o VirusScan foi instalado. Em seguida, digite `scan /?` para exibir uma lista de opções e descrições da maneira como podem ser utilizadas.

NOTA: Ao especificar um nome de arquivo como parte de uma opção de linha de comando, você deve incluir o caminho completo do arquivo, caso ele não esteja localizado no diretório em que o VirusScan esteja instalado.

Opção da Linha de comando	Descrição
`/?` ou `/HELP`	Não examina. Em vez disso, exibe um lista de opções de linha de comando do VirusScan seguidas por uma breve descrição. Use apenas uma dessas opções na linha de comando (sem outras opções).
`/ADL`	Examina todas as unidades locais (incluindo as unidades compactadas, de CD-ROM e PCMCIA, mas não os disquetes), além das especificadas na linha de comando. Para examinar as unidades local e de rede, use /ADL e /ADN na mesma linha de comando.
`/ADN`	Examina todas as unidades de rede em busca de vírus, além das especificadas na linha de comando. Para examinar as unidades local e de rede, use /ADL e /ADN na mesma linha de comando.

Opção da Linha de comando	Descrição
/AF nome do arquivo	Armazena códigos de validação/recuperação em *nome do arquivo.* Ajuda a detectar vírus novos ou desconhecidos. A opção /AF registra dados de validação e recuperação para os arquivos executáveis, o setor de inicialização e o Registro de inicialização principal em disco rígido ou disquete, no arquivo que você especifica. O arquivo de registro contém 89 bytes por arquivo validado. Deve ser especificado um *nome de arquivo* que possa incluir o caminho completo. Se o caminho de destino for uma unidade de rede, você deve ter direitos para criar e excluir arquivos nessa unidade. Se *nome do arquivo* já existir, o VirusScan o atualizará. A opção /AF adiciona aproximadamente 300% ao tempo da varredura. **NOTA:** /AF executa a mesma função que /AV, mas armazena os seus dados em um arquivo separado, em vez de alterar os arquivos executáveis. A opção /AF não armazena informações sobre o Registro de inicialização principal ou o setor de inicialização da unidade que está sendo examinada.
/ALERTPATH <diretório>	Designa o <diretório> como um caminho de rede monitorado pelo NetShield para Alerta Centralizado.
/ALL	Sobrepõe as configurações padrão ao examinar todos os arquivos. Essa opção aumenta substancialmente o tempo necessário de varredura. Use-a se tiver encontrado um vírus ou suspeita que haja algum. **NOTA:** A lista de extensões dos executáveis padrão é diferente daquela encontrada nas versões anteriores do VirusScan.
/APPEND	Utilizada com /REPORT, anexa o texto da mensagem de relatório ao arquivo especificado, se houver. Caso contrário, a opção /REPORT sobrepõe o arquivo de relatório especificado, se houver.

Opção da Linha de comando	Descrição
/AV	Para ajudar a detectar e a recuperar o sistema das infecções por vírus novos ou desconhecidos, a opção /AV adiciona dados de validação e recuperação a cada arquivo executável padrão (.EXE, .COM, .SYS, .BIN, .OVL e .DLL), aumentando o seu tamanho em 98 bytes. Para atualizar arquivos em uma unidade de rede compartilhada, você deve ter direitos de acesso para atualização. Para excluir os arquivos automodificadores ou autoverificadores, e arquivos danificados que possam causar alarmes falsos, use a opção /EXCLUDE. A utilização de qualquer uma das opções /AV, /CV ou /RV juntas na mesma linha de comando retorna um erro. **NOTA:** A opção /AV não armazena informações sobre o Registro de inicialização principal ou o setor de inicialização da unidade que está sendo examinada.
/BOOT	Examina somente o setor de inicialização e o Registro de inicialização principal na unidade especificada.
/CF nome do arquivo	Ajuda a detectar vírus novos ou desconhecidos. Verifica os dados de validação armazenados pela opção /AF em *nome do arquivo*. Se um arquivo ou área do sistema forem alterados, o VirusScan relata que pode ter ocorrido uma infecção por vírus. A opção /CF acrescenta mais 250% ao tempo da varredura. O uso de qualquer uma das opções /AF, /CF ou /RF juntas na mesma linha de comando retorna um erro. **NOTA:** Alguns PCs da Hewlett-Packard e Zenith mais antigos modificam o setor de inicialização sempre que o sistema é inicializado. Se você usar a opção /CF, o VirusScan relatará continuamente que o setor de inicialização foi modificado mesmo que nenhum vírus tenha sido detectado. Verifique o manual de referência de seu computador para determinar se tem código de inicialização automodificado.
/CLEAN	Limpa arquivos infectados.
/CLEANDOC	Limpa vírus de arquivos de documentos do Word infectados.
/CLEANDOCALL	Limpa todas as macros de arquivos de documentos do Word infectados.
/CONTACTFILE nome do arquivo	Identifica um arquivo que contém uma seqüência de caracteres da mensagem a ser exibida quando um vírus for encontrado. Esta opção é útil principalmente em ambientes de rede, pois você pode facilmente manter o texto da mensagem em um arquivo central, sem precisar colocá-la em cada estação de trabalho. Qualquer caractere é válido exceto uma barra inclinada para a esquerda (\). As mensagens que começam com uma barra inclinada para a direita (/) ou um hífen (-) devem ser colocadas entre aspas.

Opção da Linha de comando	Descrição
/CV	Ajuda a detectar vírus novos ou desconhecidos. Verifica os dados de validação adicionados pela opção /AV. Se um arquivo for modificado, o VirusScan relata que pode ter ocorrido uma infecção por vírus. A opção /CV adiciona mais 50%, aproximadamente, ao tempo da varredura. O uso de qualquer uma das opções /AV, /CV ou /RV juntas na mesma linha de comando retorna um erro. **NOTA:** A opção /CV não verifica se há alterações no setor de inicialização.
/DEL	Exclui os arquivos infectados.
/EXCLUDE nome do arquivo	Exclui quaisquer arquivos listados em*nome do arquivo* da varredura. Esta opção permite excluir arquivos das validações /AF e /AV, e das verificações /CF e /CV. Os arquivos automodificadores ou autoverificadores podem causar um alarme falso durante uma varredura.
/FAST	Acelera a varredura. Reduz em cerca de 15% o tempo de varredura. Usando a opção /FAST, o VirusScan examina uma parte menor de cada arquivo em busca de vírus. O uso da opção /FAST pode não detectar algumas infecções encontradas em uma varredura mais abrangente (porém mais lenta). Não use esta opção se tiver encontrado um vírus ou suspeitar que haja algum.
/FORCE	Limpa os vírus da tabela de partições sobrepondo ao registro de inicialização do disco com um Registro de inicialização principal.
/FREQUENCY horas	O intervalo de horas entre varreduras subseqüentes bem-sucedidas (Exemplo: /FREQUENCY 1). Nos ambientes onde o risco de infecção viral é muito baixo, use esta opção para evitar varreduras desnecessárias ou muito freqüentes. Quanto menor o número de *horas* especificado, maior a freqüência de varreduras e maior a sua proteção contra infecções.
/LOAD nome do arquivo	Executa uma varredura usando as informações salvas em*nome do arquivo*. Você pode armazenar todas as definições personalizadas em um arquivo de configuração separado (um arquivo de texto ASCII) e, em seguida, usar a opção /LOAD para carregá-las desse arquivo.

Opção da Linha de comando	Descrição
/LOCK	Pára o sistema para interromper infecções adicionais, caso o VirusScan encontre um vírus. A opção /LOCK é adequada para ambientes de rede altamente vulneráveis, como laboratórios de informática de uso aberto. Se você usar a opção /LOCK, recomendamos que adicione a opção /CONTACTFILE para informar aos usuários o que fazer ou quem contactar caso um vírus seja encontrado e o sistema trave.
/LOG	Registra a hora e a data em que o VirusScan for executado através da atualização ou criação de um arquivo chamado SCAN.LOG no diretório raiz da unidade de disco atual.
/MANY	Examina diversos disquetes consecutivamente em uma única unidade. O VirusScan lhe solicita cada disquete. Uma vez estabelecido um sistema isento de vírus, use esta opção para verificar vários disquetes rapidamente. O programa VirusScan deve residir em um disco que não seja removido durante a varredura. Por exemplo, se estiver examinando disquetes na unidade A:, e você estiver executando o programa a partir de um disquete nessa mesma unidade A:, o programa ficará indisponível logo que o disquete for removido para ser substituído por outro. O seguinte comando provoca um erro durante sua execução: a:\scan a: /many
/MAXFILESIZE xxx.x	Examina apenas arquivos com tamanho até xxx.x megabytes.
/MEMEXCL	Exclui a área da memória da varredura. (O padrão é A000-FFFF, 0000=Examinar tudo.) Esta opção de linha de comando foi acrescentada para impedir que o VirusScan verifique áreas da memória superior que possam conter hardware mapeado na memória e causar alarmes falsos.
/MOVE diretório	Move todos os arquivos infectados, encontrados durante uma varredura para o diretório especificado. Para preservar a estrutura do diretório e da unidade, esta opção não terá efeito caso o Registro de inicialização principal ou o setor de inicialização estejam infectados, uma vez que estes não são, de fato, arquivos.
/NOBEEP	Desativa o alerta audível emitido sempre que o VirusScan encontra um vírus.
/NOBREAK	Desativa o CRTL-C e CRTL-BREAK durante as varreduras. Os usuários não serão capazes de interromper as varreduras em andamento usando CRTL-C ou CRTL-BREAK. Use esta opção junto com a opção /LOG para criar uma trilha de auditoria eficiente das varreduras regularmente planejadas.

Opção da Linha de comando	Descrição
/NOCOMP	Ignora a verificação de executáveis compactados, criados com os programas de compactação de arquivos LZEXE ou PKLITE. Reduz o tempo de varredura quando um exame completo não for necessário. Caso contrário, como padrão, o VirusScan verifica os arquivos executáveis ou autodescompactáveis, que foram criados com os programas de compactação de arquivos LZEXE ou PKLITE. O VirusScan descompacta cada arquivo da memória e o examina em busca de assinaturas de vírus, o que demora, mas resulta em uma varredura mais completa. Se você usar a opção /NOCOMP, o VirusScan não examinará o conteúdo dos arquivos compactados em busca de vírus, embora possa procurar modificações nesses arquivos, se tiverem sido validadas usando os códigos de validação/recuperação.
/NODDA	Sem acesso direto a disco. Impede que o VirusScan acesse o registro de inicialização. Este recurso foi adicionado para permitir que o VirusScan seja executado no Windows NT. Você pode precisar usar esta opção em algumas unidades orientadas por dispositivos.
/NODOC	Não examina os arquivos de documentos do Word.
/NOEMS	Impede que o VirusScan use a memória expandida (LIM EMS 3.2), assegurando que a EMS fique disponível para outros programas.
/NOEXPIRE	Desativa a mensagem “data de validade” caso os arquivos de dados do VirusScan estejam vencidos.
/NOMEM	Reduz o tempo de varredura, omitindo todas as verificações de memória em busca de vírus. Use a opção /NOMEM apenas quando estiver absolutamente seguro de que o seu computador não contém vírus. O VirusScan poderá verificar a memória do sistema em busca de todos os vírus críticos de computador conhecidos, que possam residir na memória. Além da memória principal de 0KB a 640KB, o VirusScan verifica a memória do sistema de 640KB a 1088KB que possa ser utilizada por vírus de computador em sistemas 286 e posteriores. A memória acima de 1088KB não é acessada diretamente pelo processador e, portanto, não é suscetível a vírus.

Opção da Linha de comando	Descrição
/PAUSE	Ativa a pausa de tela. Se você especificar a opção /PAUSE, o aviso “Pressione qualquer tecla para continuar ” aparecerá quando o VirusScan preencher uma tela com mensagens (por exemplo, quando estiver usando as opções /SHOWLOG ou /VIRLIST). Caso contrário, como padrão, o VirusScan preenche e rola a tela continuamente, o que permite ao VirusScan ser executado em computadores com diversas unidades ou que tenham infecções sérias sem que necessite do seu acompanhamento. Recomendamos que você omita a opção /PAUSE quando mantiver um registro das mensagens do VirusScan, utilizando as opções de relatório (/REPORT, /RPTCOR, /RPTMOD e /RPTERR).
/PLAD	Preserva as últimas datas de acesso (somente em unidades de disco patenteadas). Impede a alteração do atributo da última data de acesso para os arquivos armazenados em uma unidade de uma rede patenteada. Normalmente, essas unidades de rede atualizam a última data de acesso quando o VirusScan abre e examina um arquivo. Entretanto, alguns sistemas de backup em fita usam esta última data de acesso para decidir se devem fazer um backup do arquivo. Use a opção /PLAD para assegurar que a última data de acesso não será alterada como resultado da varredura.
/REPORT nome do arquivo	Cria um relatório de arquivos infectados e erros do sistema. Salva a saída do VirusScan em *nome do arquivo* no formato de arquivo de texto ASCII. Se *nome do arquivo* já existir, a opção /REPORT o apaga e substitui (ou, se for usado /APPEND, adiciona as informações de relatório no final do arquivo existente). Pode ser incluída a unidade e o diretório de destino (como D:\VSREPRT\ALL.TXT), mas se a unidade de destino for de rede, você deverá ter direitos para criar e excluir arquivos nessa unidade. Podem ser usadas também opções /RPTALL, /RPTCOR, /RPTMOD e /RPTERR para adicionar arquivos examinados, danificados, modificados e erros do sistema no relatório.
/RF nome do arquivo	Remove dados de recuperação e validação de*nome do arquivo* criados pela opção /AF. Se *nome do arquivo* residir em uma unidade de rede compartilhada, você deve poder excluir os arquivos dessa unidade. O uso de qualquer uma das opções /AF, /CF ou /RF juntas na mesma linha de comando retorna um erro.
/RPTALL	Adiciona uma lista de arquivos examinados ao arquivo de relatório (usada com a opção /REPORT).

Opção da Linha de comando	Descrição
/RPTCOR	Quando usada com a opção /REPORT, adiciona os nomes dos arquivos danificados ao arquivo de relatório. Um arquivo danificado pode ser um arquivo infectado por um vírus. Você pode usar a opção /RPTCOR com as opções /RPTMOD e /RPTERR na mesma linha de comando. **NOTA:** Podem ocorrer leituras falsas em alguns arquivos que requerem um arquivo de sobreposição ou outro executável para funcionarem corretamente (ou seja, arquivos que não são autoexecutáveis).
/RPTERR	Adiciona uma lista de erros do sistema ao arquivo de relatório. Esta opção é usada junto com a opção /REPORT. Os erros do sistema incluem problemas de leitura ou gravação para um disquete ou disco rígido, problemas de sistemas de arquivo ou rede, problemas na criação de relatórios e outros relacionados ao sistema. Você pode usar a opção /RPTERR com /RPTCOR e /RPTMOD na mesma linha de comando.
/RPTMOD	Adiciona uma lista de arquivos modificados ao arquivo de relatório. Esta opção é usada junto com a opção /REPORT. O VirusScan identifica os arquivos modificados quando os códigos de validação/recuperação não coincidem (usando as opções /CF ou /CV). Você pode usar a opção /RPTMOD com /RPTCOR e /RPTERR na mesma linha de comando.
/RV	Remove os dados de validação e recuperação dos arquivos validados com a opção /AV. Para atualizar os arquivos em uma unidade de rede compartilhada, você deve ter direitos de acesso para atualizá-los. O uso de qualquer uma das opções /AV, /CV ou /RV juntas na mesma linha de comando retorna um erro.
/SHOWLOG	Exibe o conteúdo do SCAN.LOG. O SCAN.LOG armazena a hora e data em que o VirusScan estiver sendo executado através da atualização ou criação de um arquivo denominado SCAN.LOG localizado no diretório atual, além da data e hora das varreduras anteriores, gravadas nesse arquivo usando a chave /LOG. O arquivo SCAN.LOG contém texto e formatação especial. Para fazer uma pausa quando a tela for preenchida com mensagens, especifique a opção /PAUSE.

Opção da Linha de comando	Descrição
/SUB	Examina os subdiretórios em um diretório. Como padrão, quando você especifica um diretório para ser examinado em vez de uma unidade, o VirusScan examinará somente os arquivos nele contidos e não os seus subdiretórios. Use a opção /SUB para examinar todos os subdiretórios de qualquer diretório especificado. Não use a opção /SUB ao examinar uma unidade inteira.
/VIRLIST	Exibe o nome e uma breve descrição de cada vírus detectado pelo VirusScan. Para fazer uma pausa quando a tela for preenchida com mensagens, especifique a opção /PAUSE. Use somente a opção /VIRLIST, ou junto com a opção /PAUSE, na linha de comando. Você pode salvar a lista de nomes e descrições de vírus em um arquivo através do redirecionamento da saída do comando. Por exemplo, no DOS, digite: scan /virlist > nome do arquivo.txt **NOTA:** Como o VirusScan pode detectar muitos vírus este arquivo terá mais de 250 páginas.

Níveis de erro do DOS no VirusScan

Quando o VirusScan é executado em um ambiente DOS, é configurado um nível de erro do DOS. Você pode usar o ERRORLEVEL em arquivos de lote para atuar de modos diferentes com base nos resultados da varredura.

NOTA: Veja a sua documentação do sistema operacional DOS para obter mais informações.

O VirusScan pode retornar os seguintes níveis de erro:

ERRORLEVEL	Descrição
0	Não ocorreram erros, nenhum vírus foi encontrado.
1	Ocorreu um erro ao acessar o arquivo (leitura ou gravação).
2	Um arquivo de dados do VirusScan está danificado.
3	Ocorreu um erro no acesso a um disco (leitura ou gravação).
4	Ocorreu um erro no acesso ao arquivo criado com a opção /AF; o arquivo foi danificado.
5	Memória insuficiente para carregar um programa ou completar uma operação.

ERRORLEVEL	Descrição
6	Ocorreu um erro interno do programa (erro de falta de memória).
7	Ocorreu um erro no acesso ao arquivo de mensagem internacional (MCAFEE.MSG).
8	Falta um arquivo necessário para executar o VirusScan, como o SCAN.DAT.
9	Foram especificadas opções ou argumentos de opções incompatíveis ou irreconhecíveis na linha de comando.
10	Foi encontrado um vírus na memória.
11	Ocorreu um erro interno do programa.
12	Ocorreu um erro ao tentar remover um vírus, como “não foi encontrado o arquivo CLEAN.DAT”, ou o VirusScan não pôde remover o vírus.
13	Foi encontrado um ou mais vírus no Registro de inicialização principal, no setor de inicialização ou nos arquivos.
14	O arquivo SCAN.DAT está desatualizado; atualize a versão dos arquivos de dados do VirusScan.
15	A autoverificação do VirusScan falhou; deve estar infectado ou danificado.
16	Ocorreu um erro no acesso a uma unidade ou arquivo específico.
17	Não foi especificada uma unidade, diretório ou arquivo; não há nada a examinar.
18	Foi modificado um arquivo validado (opções /CF ou /CV).
19-99	Reservado.
100+	Erro do sistema operacional; o VirusScan adiciona 100 ao número original.
102	Foi usadoCRTL-C ou CRTL-BREAK para interromper a varredura. (Você pode desativar CRTL-Cou CRTL-BREAK com a opção de linha de comando /NOBREAK.)

Formato de arquivo VSH

O arquivo VSH é um arquivo de texto de configuração, formatado de modo semelhante ao arquivo INI do Windows, que descreve as configurações do VShield. Cada variável no arquivo tem um nome seguido de um sinal de igual (=) e por um valor. Os valores definem as definições selecionadas para a configuração do VShield. As variáveis são organizadas em sete grupos: General (Geral), DetectionOptions (Opções de detecção), AlertOptions (Opções de alerta), ActionOptions (Opções de ação), ReportOptions (Opções de relatório), SecurityOptions (Opções de segurança) e ExclusionOptions (Opções de exclusão). Para editar o arquivo VSH, abra-o com um editor de texto, como o Bloco de Notas.

NOTA: Nas variáveis Booleanas, os valores possíveis são 0 e 1. O valor 0 instrui o VirusScan a desativar a configuração enquanto 1 informa que está ativada.

General

Variável	Descrição
bLoadAtStartup	Tipo: Booleana (1/0) Define se o VShield pode ser carregado na inicialização do sistema Valor padrão: 1
bCanBeDisabled	Tipo: Booleana (1/0) Define se o VShield pode ser desativado Valor padrão: 1
bShowTaskbarIcon	Tipo: Booleana (1/0) Define se o ícone do VShield é exibido na barra de tarefas Valor padrão: 1
bNoSplash	Tipo: Booleana (1/0) Instrui o VirusScan a não exibir a tela inicial do logotipo do produto ao inicializar o programa Valor padrão: 0

DetectionOptions

Variável	Descrição
szProgramExtensions	Tipo: Seqüência de caracteres Define as extensões a serem examinadas Valor padrão: EXE COM DO? XL?
szDefaultProgramExtensions -	Tipo: Seqüência de caracteres Define as extensões de programa padrão a serem utilizadas durante a configuração da varredura Valor padrão: EXE COM DO? XL?
bScanOnExecute	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando são executados Valor padrão: 1
bScanOnOpen	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando são abertos Valor padrão: 1
bScanOnCreate	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando são criados Valor padrão: 1
bScanOnRename	Tipo: Booleana (1/0) Instrui o VShield a examinar os arquivos quando são renomeados Valor padrão: 1
bScanOnBootAccess	Tipo: Booleana (1/0) Instrui o VShield a examinar o registro de inicialização de uma unidade de disco quando for acessada pela primeira vez Valor padrão: 1
bScanAllFiles	Tipo: Booleana (1/0) Instrui o programa a examinar o conteúdo de todos os arquivos Valor padrão: 0
bScanCompressed	Tipo: Booleana (1/0) Instrui o programa a examinar o conteúdo dos arquivos compactados (PkLite, LZEXE) Valor padrão: 1

AlertOptions

Variável	Descrição
bNetworkAlert	Tipo: Booleana (1/0) Instrui o VShield a enviar um alerta de rede para uma pasta monitorada pelo NetShield para Alerta Centralizado. Valor padrão: 0
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica o caminho que está monitorado pelo NetShield para Alerta Centralizado. Valor padrão: Nenhum

ActionOptions

Variável	Descrição
szCustomMessage	Tipo: Seqüência de caracteres Define uma mensagem personalizada que será exibida quando for encontrado um vírus, se a ação for configurada como Solicitar ação Valor padrão: Possível Vírus Detectado
szMoveToFolder	Tipo: Seqüência de caracteres Define a pasta para a qual os arquivos devem ser movidos Valor padrão: \Infectado
uVshieldAction	Tipo: Número inteiro (1-5) Instrui oVShield a executar a ação especificada quando um vírus for detectado Valores possíveis: 1 - Solicitar ação 2 - Mover arquivos infectados para uma pasta 3 - Limpar arquivos infectados automaticamente (Nega acesso caso os arquivos não possam ser limpos) 4 - Excluir arquivos infectados automaticamente 5 - Negar acesso para arquivos infectados Valor padrão: 1
bButtonClean	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário uma opção de limpeza de arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1

Variável	Descrição
bButtonDelete	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de excluir o arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonExclude	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de eliminar um arquivo, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonStop	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de negar acesso ao arquivo infectado, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bButtonContinue	Tipo: Booleana (1/0) Instrui o VShield a fornecer ao usuário a opção de continuar com o evento interrompido, se a opção Solicitar ação for selecionada e um vírus detectado Valor padrão: 1
bDisplayMessage	Tipo: Booleana (1/0) Define se a mensagem personalizada deve ser exibida quando um vírus for detectado Valor padrão: 0

ReportOptions

Variável	Descrição
szLogFileName	Tipo: Seqüência de caracteres Define o nome do arquivo de registro Valor padrão: C:\McAfee\Viruscan\Vshlog.txt
bLogToFile	Tipo: Booleana (1/0) Define se os resultados da varredura devem ser incluídos em um arquivo de registro Valor padrão: 1
bLimitSize	Tipo: Booleana (1/0) Define se o tamanho do arquivo deve ser limitado Valor padrão: 1

Variável	Descrição
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro em quilobytes Valor padrão: 100
bLogDetection	Tipo: Booleana (1/0) Define se os resultados da varredura devem ser registrados Valor padrão: 1
bLogClean	Tipo: Booleana (1/0) Define se os resultados da limpeza devem ser registrados Valor padrão: 1
bLogDelete	Tipo: Booleana (1/0) Define se as operações de exclusão do arquivo infectado devem ser registradas Valor padrão: 1
bLogMove	Tipo: Booleana (1/0) Define se as operações de movimentação do arquivo infectado devem ser registradas Valor padrão: 1
bLogSettings	Tipo: Booleana (1/0) Define se as configurações da sessão devem ser registradas ao desligar o sistema Valor padrão: 1
bLogSummary	Tipo: Booleana (1/0) Define se o resumo da sessão deve ser registrado ao desligar o sistema Valor padrão: 1
bLogDateTime	Tipo: Booleana (1/0) Define se a data e a hora de um evento devem ser registradas Valor padrão: 1
bLogUserName	Tipo: Booleana (1/0) Define se o nome do usuário deve ser registrado Valor padrão: 1

SecurityOptions

Variável	Descrição
szPasswordProtect	Tipo: Seqüência de caracteres Esta opção não pode ser configurada pelo usuário. Valor padrão: 0
szPasswordCRC	Tipo: Seqüência de caracteres Esta opção não pode ser configurada pelo usuário. Valor padrão: 0

ExclusionOptions

Variável	Descrição
szExclusionsFileName	Tipo: Seqüência de caracteres Esta opção não pode ser configurada pelo usuário.
NumExcludedItems	Tipo: Número inteiro (0-n) Define o número de itens excluídos de uma varredura ao acessar Valor padrão: 0
ExcludedItem_x, onde x é um índice com base zero	Tipo: Seqüência de caracteres Instrui o VShield a excluir o item da varredura ao acessar Valor padrão: \Recycled|*.*|1|1 * * A seqüência é separada em campos por uma barra vertical (|): Campo 1 - Parte relativa à pasta do item a ser excluído. Deixe-a em branco para um único arquivo em qualquer local do sistema. Campo 2 - Parte relativa à pasta do item a ser excluído. Deixe-a em branco se a pasta for excluída sem um nome do arquivo. Campo 3 - Número inteiro (1-3) Valores possíveis: 1 - Exclui da varredura de arquivo ao acessar 2 - Exclui da varredura de registro de inicialização 3 - Exclui da varredura de registro de inicialização e de arquivo ao acessar Campo 4 - Booleana (1/0) Valores possíveis: 1 - Instrui o VShield a excluir as subpastas do item eliminado 2 – Instrui o VShield a não excluir as subpastas

Formato de arquivo VSC

A extensão .VSC designa um arquivo de texto de configuração, semelhante no formato ao arquivo INI do Windows, que descreve as configurações do VirusScan. Cada variável nesse arquivo tem um nome seguido por um sinal de igual (=) e por um valor. Esses valores definem quais definições foram selecionadas para a configuração do VirusScan. As variáveis estão organizadas em oito grupos: ScanOptions (Opções de varredura), DetectionOptions (Opções de detecção), AlertOptions (Opções de alerta), ActionOptions (Opções de ação), ReportOptions (Opções de relatório), ScanItems (Itens de varredura), SecurityOptions (Opções de segurança) e ExcludedItems (Itens de exclusão). Para editar o arquivo VSC, abra-o com um editor de texto, como o Bloco de Notas.

NOTA: Nas variáveis Booleanas, os valores possíveis são 0 e 1. O valor 0 instrui o VirusScan a desativar a configuração, enquanto 1 indica que a configuração está ativada.

ScanOptions

Variável	Descrição
bAutoStart	Tipo: Booleana (0/1) Instrui o VirusScan a iniciar automaticamente a varredura ao ser aberto Valor padrão: 0
bAutoExit	Tipo: Booleana (0/1) Instrui o VirusScan a sair automaticamente ao terminar a varredura Valor padrão: 0
bAlwaysExit	Tipo: Booleana (0/1) NEED DESCRIPTION HERE Valor padrão: 0
bSkipMemoryScan	Tipo: Booleana (0/1) Instrui o VirusScan a ignorar a memória durante a varredura Valor padrão: 0

Variável	Descrição
bSkipBootScan	Tipo: Booleana (0/1) Instrui o VirusScan a ignorar o setor de inicialização durante a varredura Valor padrão: 0
bSkipSplash	Tipo: Booleana (0/1) Instrui o VirusScan a não exibir a janela do logotipo do VirusScan na inicialização Valor padrão: 0

DetectionOptions

Variável	Descrição
bScanAllFiles	Tipo: Booleana (0/1) Instrui o VirusScan a examinar todos os tipos de arquivos Valor padrão: 0
bScanCompressed	Tipo: Booleana (0/1) Instrui o VirusScan a examinar o conteúdo dos arquivos compactados Valor padrão: 1
szProgramExtensions	Tipo: Seqüência de caracteres Especifica quais extensões de arquivos o VirusScan examinará Valor padrão: EXE COM DO? XL?
szDefaultProgramExtensions	Tipo: Seqüência de caracteres Especifica o valor padrão para szProgramExtensions Valor padrão: EXE COM DO? XL?

AlertOptions

Variável	Descrição
bNetworkAlert	Tipo: Booleana (0/1) Instrui o VirusScan a enviar um arquivo (.ALR) de alerta a um caminho de rede monitorado pelo NetShield para Alerta Centralizado quando um vírus for encontrado Valor padrão: 0

Variável	Descrição
bSoundAlert	Tipo: Booleana (0/1) Instrui o VirusScan a soar um alerta audível quando um vírus for detectado Valor padrão: 1
szNetworkAlertPath	Tipo: Seqüência de caracteres Especifica o caminho do alerta de rede que está sendo monitorado pelo NetShield para Alerta Centralizado. A pasta indicada por este caminho deve conter o arquivo de Alerta Centralizado, CENTALERT.TXT Valor padrão: Nenhum

ActionOptions

Variável	Descrição
bDisplayMessage	Tipo: Booleana (0/1) Instrui o VirusScan a exibir uma mensagem ao detectar um vírus Valor padrão: 0
ScanAction	Tipo: Número inteiro (0-5) Instrui o ViruScan a agir da maneira especificada quando um vírus for detectado Valores possíveis: 0 - Solicitar ação 1 - Mover automaticamente 2 - Limpar automaticamente 3 - Eliminar automaticamente 4 - Continuar Valor padrão: 0
bButtonClean	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Limpar se ScanAction=0 Valor padrão: 1
bButtonDelete	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Eliminar se ScanAction=0 Valor padrão: 1
bButtonExclude	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Excluir se ScanAction=0 Valor padrão: 1

Variável	Descrição
bButtonMove	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Mover se ScanAction=0 Valor padrão: 1
bButtonContinue	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Continuar se ScanAction=0 Valor padrão: 1
bButtonStop	Tipo: Booleana (0/1) Instrui o VirusScan a exibir o botão Parar se ScanAction=0 Valor padrão: 1
szMoveToFolder	Tipo: Seqüência de caracteres Indica para onde os arquivos infectados devem ser movidos Valor padrão: \Infectado
szCustomMessage	Tipo: Seqüência de caracteres Indica o texto da mensagem a ser exibido quando for encontrado um vírus Valor padrão: Possível Vírus Detectado

ReportOptions

Variável	Descrição
bLogToFile	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as atividades de varredura em um arquivo Valor padrão: 1
bLimitSize	Tipo: Booleana (0/1) Instrui o VirusScan a limitar o tamanho do arquivo de registro Valor padrão: 1
uMaxKilobytes	Tipo: Número inteiro (10-999) Define o tamanho máximo do arquivo de registro, em kilobytes Valor padrão: 10
bLogDetection	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a detecção de vírus Valor padrão: 1
bLogClean	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a limpeza de vírus Valor padrão: 1

Variável	Descrição
bLogDelete	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as exclusões de arquivos Valor padrão: 1
bLogMove	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as movimentações de arquivos Valor padrão: 1
bLogSettings	Tipo: Booleana (0/1) Instrui o VirusScan a registrar as configurações de sessão Valor padrão: 1
bLogSummary	Tipo: Booleana (0/1) Instrui o VirusScan a registrar os resumos de sessão Valor padrão: 1
bLogDateTime	Tipo: Booleana (0/1) Instrui o VirusScan a registrar a data e hora da atividade de varredura Valor padrão: 1
bLogUserName	Tipo: Booleana (0/1) Instrui o VirusScan a registrar o nome do usuário Valor padrão: 1
szLogFileName	Tipo: Seqüência de caracteres Especifica um caminho para o arquivo de registro Valor padrão: C:\McAfee\Viruscan\VSCLOG.TXT

ScanItems

Variável	Descrição
ScanItem_x, onde x é um índice de base zero	Tipo: Seqüência de caracteres Instrui o VirusScan a examinar o item Valor padrão: C:|1 * *A seqüência é separada em campos por uma barra vertical (|): Campo 1- Caminho do item a ser examinado. Campo 2 - Booleana (1/0) Valores possíveis: 1 – Instrui o VirusScan a examinar as subpastas do item 2 – Instrui o VirusScan a não examinar as subpastas do item

SecurityOptions

Variável	Descrição
szPasswordProtect	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0
szPasswordCRC	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0
szSerialNumber	Tipo: Seqüência de caracteres Esta variável não pode ser configurada pelo usuário Valor padrão: 0

ExcludedItems

Variável	Descrição
NumExcludeItems	Tipo: Número inteiro (0-n) Define o número de itens que serão excluídos da varredura Valor padrão: 1
ExcludedItem_x, onde x é um índice de base zero	Tipo: Seqüência de caracteres Instrui o VirusScan a excluir o item da varredura Valor padrão: \Recycled|*.*|1|1 * * A seqüência é separada em campos por uma barra vertical (|): Campo 1 - Parte relativa à pasta do item a ser examinado. Deixar em branco para um único arquivo em qualquer lugar do sistema. Campo 2 - Parte relativa ao arquivo do item a ser examinado. Deixar em branco se uma pasta for examinada sem um nome de arquivo. Campo 3 - Número inteiro (1-3) Valores possíveis: 1 - Exclui da varredura de arquivo 2 - Exclui da varredura do setor de inicialização 3 - Exclui da varredura da varredura do registro de inicialização e de arquivo Campo 4 - Booleana (1/0) Valores possíveis: 1 - Instrui o VirusScan a ignorar as subpastas do item excluído 2 - Instrui o VirusScan a não excluir as subpastas

Glossário

alarme falso	Relatar a infecção por um vírus quando não há nenhum.
arquivo compactado	Um arquivo que foi compactado usando um utilitário de compactação de arquivos, como o PKZIP. Veja também“executável compactado.”
arquivo danificado	Um arquivo que foi danificado irrecuperavelmente por um vírus , por exemplo. detecção
arquivo infectado	Um arquivo contaminado por um vírus.
arquivo modificado	Um arquivo que foi modificado após os códigos de validação terem sido adicionados, possivelmente por um vírus.
BIOS	Um chip de memória somente para leitura que contém as instruções codificadas para a utilização do hardware, como um teclado ou monitor. Sempre presente nos computadores portáteis, um BIOS (ROM de inicialização) não é susceptível a infecção (diferente do setor de inicialização de um disco). Alguns chips de BIOS contêm recursos antivírus que podem gerar um alarme falso, falha de instalação e outros problemas.
Bloco de memória superior (UMB)	Memória na faixa de 640KB a 1024KB, bem acima do limite de 640KB do DOS para a memória convencional.
códigos de recuperação	Informações que o VirusScan grava sobre um arquivo executável para recuperá-lo (repará-lo) se for danificado por um vírus. Veja também “códigos de validação.”
códigos de validação	Informações que o VirusScan grava sobre um arquivo executável para detectar uma infecção subseqüente por um vírus. Veja também “códigos de recuperação.”
desinfectar	Erradicar um vírus para que ele não possa mais espalhar-se ou causar danos a um sistema. lista de exceções
detecção	Varredura da memória e dos discos em busca de pistas indicativas da existência de vírus. Alguns métodos de detecção incluem a busca de padrões virais comuns ou cadeia de caracteres, comparação da atividade suspeita do arquivo com a atividade de vírus conhecidos e monitoração dos arquivos em busca de alterações não autorizadas.
disco de inicialização	Um disquete protegido contra gravação que contém o sistema do computador e os arquivos de inicialização. Você pode usar esse disquete para iniciar o seu computador. É importante usar um disco de inicialização livre de vírus para garantir que o computador não seja infectado.

erros do sistema	Erros que podem impedir que o VirusScan complete o seu trabalho com sucesso. A condições de erro do sistema incluem erros de formatação de disco, erros de mídia, erros de sistema de arquivos, erros de rede, erro de acesso a dispositivos e falhas de relatório.
executável (arquivo)	Um arquivo que contém instruções codificadas para serem executadas pelo computador. Os arquivos executáveis incluem programas e programas de sobreposição (códigos de programas auxiliares que não podem ser executados diretamente pelo usuário).
executável compactado	Um arquivo que foi compactado usando um utilitário de compactação de arquivos, como LZEXE ou PKLITE. Veja também "arquivo compactado."
infecção da memória	Contaminação da memória por um vírus. A única forma garantida de eliminar a infecção da memória é *desligar o seu computador,* reiniciá-lo a partir de um disquete de inicialização limpo e limpar a origem da infecção usando o VirusScan.
infecção de arquivo de sobreposição	Contaminação por vírus de um arquivo que contém código de programa auxiliar que é carregado pelo programa principal.
infecção do setor de inicialização	Contaminação do setor de inicialização por um vírus. Uma infecção do setor de inicialização é particularmente perigosa porque as informações nesse setor são carregadas primeiro na memória, *antes* que o código de proteção contra vírus possa ser executado. A única forma garantida de eliminar uma infecção do setor de inicialização é iniciar o seu computador a partir de um disquete de inicialização limpo e, em seguida, remover a infecção usando o VirusScan.
inicialização	Inicializar um computador. O computador irá carregar as instruções de inicialização a partir de uma ROM de inicialização (BIOS) ou de um setor de inicialização. Veja também "inicialização a frio" e "inicialização a quente."
inicialização a frio	Ligar um computador ou reiniciá-lo, desligar o computador, aguardar alguns segundos e religá-lo. Outros métodos de reinicialização (como pressionar um botão Reset ou CTRL+ALT+DEL) podem não remover todos os traços de uma infecção por vírus da memória. Veja também "inicialização" e "inicialização a quente."
inicialização a quente	Reiniciar (redefinir) um computador pressionando CRTL+ALT+DEL. Veja também "inicialização" e "inicialização a frio."

lista de exceções	Lista de arquivos aos quais os códigos de validação não devem ser adicionados porque contêm detecção de vírus incorporada, contêm código automodificador ou não têm a probabilidade de infecção por um vírus. Tais arquivos são normalmente ignorados na verificação de validação porque podem disparar um alarme falso.
memória	Um meio de armazenamento no qual os dados ou o código do programa são mantidos temporariamente, enquanto são utilizados pelo computador. O DOS aceita até 640KB de memória convencional. Além desse limite ela pode ser acessada como memória expandida, memória estendida ou Bloco de memória superior (UMB).
memória convencional	Até 640KB (1MB) de memória principal na qual o DOS executa os programas.
memória estendida	Memória linear acima do limite de 1MB de memória convencional. Usada freqüentemente para discos de RAM e spoolers de impressão.
memória expandida	**Memória do computador** acima do limite de 1MB de memória convencional que é acessada pela paginação de memória. Você precisa de um software especial, de acordo com uma especificação de memória expandida, para aproveitá-la.
operação de gravação	Qualquer operação na qual as informações são gravadas em um disco. Os comandos que realizam as operações de gravação incluem aqueles que salvam, movem ou copiam arquivos. Veja também “operação de leitura.”
operação de leitura	Qualquer operação na qual as informações são lidas em um disco, incluindo um disco rígido, disquete, CD-ROM ou unidade de rede. Os comandos do DOS que realizam as operações de leitura incluem DIR (listagem de diretórios), TYPE (exibe o conteúdo de um arquivo) e COPY (copia arquivos). Veja também “operação de gravação.”
programa automodificador	Software que altera os seus próprios arquivos de programas, freqüentemente para proteger-se contra vírus ou cópia ilegal. Esses programas devem ser incluídos em uma lista de exceções para evitar que essas modificações sejam relatadas como um alarme falso pelo VirusScan. erros do sistema
proteção contra gravação	Um mecanismo que protege arquivos ou discos contra alteração. Um arquivo pode ser protegido contra gravação através da alteração de seus atributos de sistema. Um disquete pode ser protegido contra gravação deslizando-se a lingüeta móvel do canto para que o orifício quadrado fique aberto (disquetes de 3,5") ou cobrindo-se a indentação do seu canto com uma etiqueta de proteção contra gravação (disquetes de 5,25").

rápida	Uma varredura mais rápida que a normal, porém menos abrangente (porque verifica uma parte menor de cada arquivo).
Registro de inicialização principal (MBR)	Uma parte de um disco rígido que contém uma tabela de partições que divide a unidade de disco em “pedaços grandes”, alguns dos quais podem ser atribuídos a sistemas operacionais diferentes do DOS. O MBR acessa o setor de inicialização.
setor de inicialização	É a parte do setor de inicialização de um disco que contém as instruções codificadas para que o sistema operacional inicie o computador.
validar	Verificar se um arquivo é autêntico e se não foi alterado. A maioria dos métodos de validação depende de uma estatística baseada em todos os dados do arquivo, que provavelmente não permanecerão constantes, caso o arquivo seja alterado.
vírus	Um programa de software que se anexa a outro programa em um disco ou se oculta na memória do computador e se espalha de um programa para outro. Os vírus podem danificar os dados, causar falhas no computador, exibir mensagens, etc.
vírus de macro	Um vírus que infecta macros, como as utilizadas por aplicativos como Microsoft Word e Excel. Embora o texto de um documento criado em um desses aplicativos não contenha nenhum código executável e, portanto, não possa ser infectado, um documento pode carregar macros infectáveis. Os vírus de macros são os segmentos que mais crescem no âmbito mundial das ameaças de vírus — o número de vírus de macros conhecido duplica a cada três meses.
vírus desconhecido	Um vírus que ainda não foi identificado e listado no SCAN.DAT. O VirusScan pode detectar vírus desconhecidos observando as alterações nos arquivos que podem resultar de infecções.
vírus polimorfo	Um vírus que tenta fugir da detecção pela alteração de sua estrutura interna ou por suas técnicas de criptografia.

Índice

E

F

I

L

M

N

O

P

R

S

T

U

V