SOFTWARE
OBRIGATÓRIO

09.

01. 02. 03. 04. 05.
06. 07. 08. 09. 10.

MCAFEE VIRUSSCAN 8

E PERSONAL FIREWALL PLUS

- PROTEJA O SEU COMPUTADOR DE VÍRUS, *SCRIPTS*, VERMES (*WORMS*), CAVALOS DE TRÓIA (*TROJANS*) E E-ESPARRELAS (*HOAXES*), CONTROLANDO TAMBÉM AS COMUNICAÇÕES ENTRE O COMPUTADOR E O EXTERIOR (REDE LOCAL OU INTERNET) COM UMA *FIREWALL*.

CENTROATLANTICO.PT

SOFTWARE
OBRIGATÓRIO

Pedro Remoaldo

MCAFEE VIRUSSCAN 8

E PERSONAL FIREWALL PLUS

- PROTEJA O SEU COMPUTADOR DE VÍRUS, *SCRIPTS*, VERMES (*WORMS*), CAVALOS DE TRÓIA (*TROJANS*) E E-ESPARRELAS (*HOAXES*), CONTROLANDO TAMBÉM AS COMUNICAÇÕES ENTRE O COMPUTADOR E O EXTERIOR (REDE LOCAL OU INTERNET) COM UMA *FIREWALL*.

CENTROATLANTICO.PT

* O leitor consente, de forma expressa, a incorporação e o tratamento dos seus dados nos ficheiros automatizados da responsabilidade do Centro Atlântico, para os fins comerciais e operativos do mesmo. O leitor fica igualmente informado sobre a possibilidade de exercer os direitos de acesso, rectificação e cancelamento dos seus dados nos termos estabelecidos na legislação vigente, na sede do Centro Atlântico, por qualquer meio escrito.

McAfee VirusScan 8
Colecção: Software obrigatório
Autor: Pedro Remoaldo
Direcção gráfica: António José Pedro
Revisão final: Centro Atlântico
Capa: António José Pedro

Av. Dr. Carlos Bacelar, 968 - Escr. 1-A - 4764-901 V. N. Famalicão
Rua da Misericórdia, 76 - 1200-273 Lisboa
Portugal
Tel. 808 20 22 21

geral@centroatlantico.pt
www.centroatlantico.pt

Impressão e acabamento: Inova
1ª edição: Dezembro de 2003

ISBN: 972-8426-82-8
Depósito legal: ……/03

Índice

I. VÍRUS - O QUE SÃO? >>

Um vírus é um programa informático que é introduzido num computador sem o conhecimento do utilizador, com a intenção de se auto-multiplicar e danificar o PC infectado, bem como outros computadores a ele ligados, quer estejam numa rede local quer sejam acessíveis via Internet. Os efeitos de um vírus variam entre poucos danos, de forma que o utilizador nem sequer se apercebe que um vírus infectou o seu computador, e a limpeza do conteúdo do disco duro, ou mesmo a inutilização do computador. Alguns vírus não têm a intenção de causar danos – podem ser apenas brincadeiras, como uma mensagem irritante que passa a vida a aparecer no ecrã. Normalmente um vírus está contido num programa, e quando esse programa é executado o vírus é activado e infecta outros programas existentes no seu computador. De cada vez que o programa infectado é executado, o vírus também é executado e desta forma espalha-se. Se o seu computador estiver infectado, pode facilmente espalhar o vírus para outros computadores que eventualmente estejam numa rede local, ou através da partilha de disquetes ou dos anexos de correio electrónico. No passado, a forma mais comum de disseminar um vírus era através da partilha de disquetes. Com a massificação do uso da Internet, este tornou-se o meio mais rápido e fácil para um vírus se disseminar.

Os vírus mais recentes são os vírus por correio electrónico. Até há pouco tempo não se podia apanhar um vírus apenas pela leitura de uma mensagem de correio electrónico. Apenas se podia ser infectado se a mensagem possuísse um anexo com vírus. O vírus "Bubbleboy" foi o primeiro vírus por correio electrónico que podia infectar um computador simplesmente pela leitura da mensagem. Outro vírus semelhante é o vírus "Kak", que também ataca sem necessidade de existir um anexo numa mensagem, inserindo-se em qualquer mensagem enviada de um sistema infectado.

Ninguém que possua um computador está imune aos vírus. Segundo a International Computer Security Association (ICSA), praticamente todas as empresas ou utilizadores já foram vítimas de uma infecção viral. Sendo que a maior parte dos vírus (80%) entraram nos computadores através do correio electrónico. E cerca de 40% dos computadores sofre uma infecção todos os anos. É de salientar que existem actualmente mais de 60 mil vírus e aparecem mensalmente cerca de 500 novos.

1.1 Tipos de vírus

Consoante o comportamento, os vírus podem ser catalogados em diversos tipos.

1.1.1 Vírus que infectam ficheiros

Estes vírus infectam preferencialmente programas com a extensão .EXE e .COM, embora também possam afectar ficheiros com as extensões .SYS, .OVL e .DLL, entre outras. Estes vírus "escondem-se" na memória do computador da primeira vez que um programa infectado é executado, e infectam qualquer programa que seja depois executado.

1.1.2 Vírus do sistema de ficheiros

Estes são vírus que modificam a tabela interna

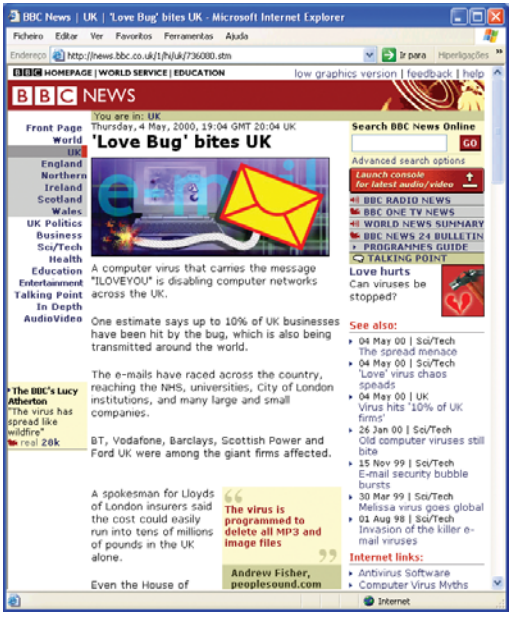
do sistema operativo que controla os ficheiros e as pastas de forma que o vírus seja carregado em memória e executado antes de cada programa que seja invocado. O programa não é afectado.

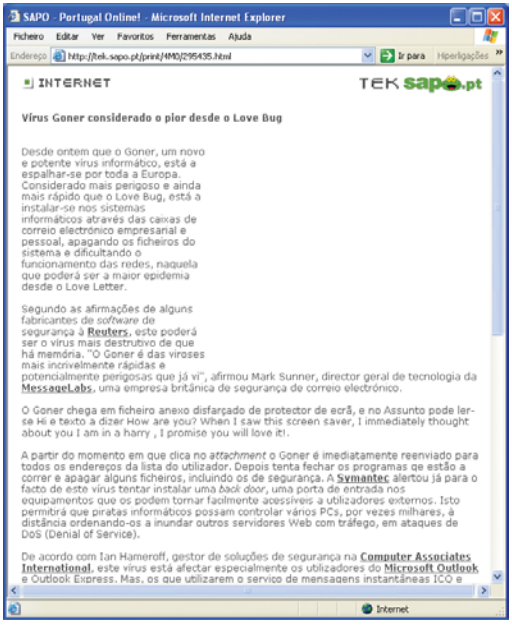
1.1.3 Vírus do sector de arranque

Vírus que infectam a área do disco duro que é lida e executada quando o computador arranca (*boot sector*). São muitas vezes disseminados através de disquetes contaminadas que são esquecidas na unidade de leitura de um computador. Quando o computador é ligado, o conteúdo da disquete é lido automaticamente e o computador é assim infectado.

1.1.4 Vírus de macros

As macros são pequenos programas que podem ser utilizados para efectuar tarefas repetitivas. Por exemplo, pode escrever uma macro no Word para adicionar de forma automática o seu nome, morada e número de telefone a documentos. As macros são automaticamente executadas quando o ficheiro a que estão anexadas é aberto. Os vírus de macro espalham-se muito mais rapidamente do que outras formas de vírus, dado que as pessoas partilham frequentemente ficheiros de dados e pensam que estes ficheiros são imunes aos vírus. Estes vírus de macros são mais comuns em ficheiros do Office, isto é, em ficheiros com a extensão *.doc*, *.xls* e *.mdb* . Por exemplo, o vírus de macro, The Love Bug (também conhecido por LoveLetter), que apareceu em Maio de 2000, teve grande impacto. O assunto da mensagem era "ILOVEYOU" e tinha anexado um ficheiro com o nome *love-letter-for-you.txt.vbs* . O vírus enviava cópias de si próprio para todos os endereços de correio electrónico existentes no livro de endereços (*address book*) do Microsoft Outlook Express.





1.1.5 Worms

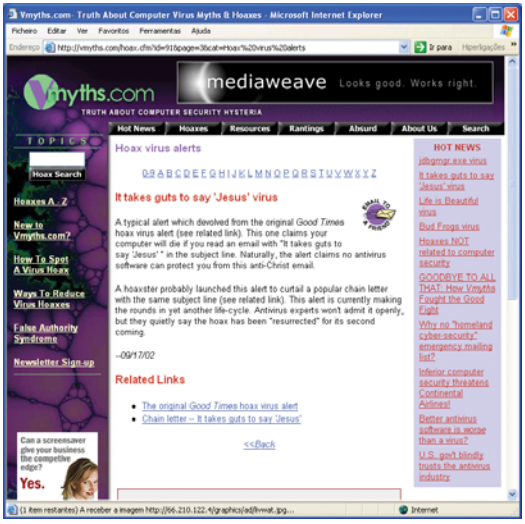
Os vermes (*worms*) residem na memória do computador e têm como actividade principal a sua reprodução (propagação) gastando todos os recursos do computador, tornando-o assim mais lento. Podem enviar cópias deles próprios para outros computadores, através do correio electrónico ou do Internet Relay Chat (IRC). Normalmente não provocam danos irreparáveis ao computador.

1.1.6 Cavalos de Tróia

Um cavalo de Tróia (*trojan horse*) é um programa impostor com propósitos maléficos, que se disfarça de aplicação benigna – por exemplo, como protectores de ecrã (*screensavers*) ou jogos. Como característica principal o facto de não se reproduzirem. Mas podem provocar danos, formatando um disco, embora a sua actividade principal seja a quebra da segurança de um computador normalmente acedendo a determinadas portas de comunicação e deixando-as acessíveis desde o exterior. Embora não possam ser considerados vírus, já que não se replicam, podem ser tão destrutivos como os vírus. São bastante difíceis de detectar.

1.1.7 Hoaxes (e-esparrelas)

Os *hoaxes* são mensagens de correio electrónico que avisam as pessoas sobre vírus inexistentes e que propagam histórias assustadoras (cibercontos do vigário). São tão comuns que as empresas de antivírus possuem páginas específicas que listam os mais comuns.
Por isso, sempre que receber uma mensagem alertando-o para o aparecimento de um novo vírus deve visitar uma destas páginas para determinar se se trata de um *hoax* ou de um vírus real. O *site* Vmyths (*http://www.vmyths.com*) disponibiliza bastante informação sobre os *hoaxes*.



1.2 Software antivírus

Para evitar as infecções de vírus, existem programas no mercado que têm a designação genérica de antivírus. O software antivírus é uma peça fundamental no combate aos vírus, *worms*, cavalos de Tróia e outros invasores indesejados que podem danificar o seu computador. As empresas mais conhecidas que produzem este tipo de programas são a McAfee, a Symantec e a Panda.
Praticamente todos os programas antivírus disponibilizam duas formas de combater os vírus:

- **On-access scanner**
  corresponde a um programa que está permanentemente activo em memória e que faz a análise de todos os ficheiros que são acedidos pelo utilizador, pelo sistema operativo ou pelas aplicações. No caso da McAfee este programa tem o nome de **ActiveShield**.

- **On-demand scanner**
  programa que é invocado pelo utilizador para efectuar uma análise a determinados ficheiros, pastas ou discos à procura de infecções virais. No caso da McAfee o programa chama-se **Scan** e a sua execução pode ser calendarizada.

DICA

Deverá manter o software antivírus permanentemente actualizado dado que, devido ao aparecimento diário de novos vírus, são necessárias permanentemente novas "vacinas". Estas vacinas são fornecidas em ficheiros que se chamam *virus definition files* e estão disponíveis nos *sites* das empresas que vendem os antivírus. A maior parte dos programas antivírus permite a actualização automática destes ficheiros quando o computador está ligado à Internet.
Porém, não basta instalar um antivírus no seu computador e actualizá-lo, é necessário que este esteja bem configurado. Por exemplo, o *on-access scanner* deve estar sempre activado, e a configuração deve prever analisar todas as mensagens de correio electrónico que sejam recebidas. Além disso, deve calendarizar uma análise do(s) disco(s) do seu computador, de forma que todos os ficheiros sejam controlados periodicamente.

1.3 Como pode um computador ser infectado?

O seu computador pode ser infectado por um vírus de várias formas:

- Através de uma disquete infectada (ou de qualquer outro suporte amovível, como um disco ZIP ou CDs);
- Abrindo um ficheiro que está infectado com um vírus de macros;
- Através de anexos de mensagens de correio electrónico infectadas com vírus de macros;
- Através de mensagens de correio electrónico infectadas;
- A partir de *applets* Java ou controlos ActiveX hostis, que são descarregados sem o saber quando navega na Web;
- A partir de programas infectados que são transferidos da Internet, de *sites* de reputação duvidosa;
- Através de programas de partilha de ficheiros na Internet (vulgo, programas P2P), como o Kazaa;
- Através de software pirateado.

Quando um vírus infecta o seu correio electrónico ou ficheiros do seu computador pode:

- Fazer sucessivas cópias de si próprio, podendo preencher o espaço livre do seu disco;
- Enviar-se para todos os contactos do seu livro de endereços (*address book*) do programa de correio electrónico;
- Formatar o seu disco duro e/ou eliminar ficheiros ou programas;
- Instalar programas escondidos, como software pirateado, que pode ser distribuído e vendido utilizando o seu computador;
- Tornar o seu computador muito lento;
- Impedir a execução de determinados programas;
- Permitir o acesso ao seu computador a partir do exterior.
- Roubar as suas palavras-passe ou outra informação pessoal existente no seu computador.

A maior parte dos vírus (cerca de 95%) não fazem mais do que replicar-se e alguma actividade trivial, como emitir um som quando utiliza o teclado, ou apresentar uma mensagem no ecrã. Há algum tempo atrás o vírus "Stoned" era o mais comum (25% das infecções) e não fazia mais do que apresentar a mensagem "Your PC is now Stoned!" no ecrã. O vírus "Italian" apresentava uma bola aos saltos no ecrã, enquanto o vírus "Cascade" fazia com que as letras caíssem para o fundo do ecrã. O problema é que algumas variantes posteriores destes vírus começaram a criar graves problemas.
Todos os vírus são catalogados pelas empresas que vendem programas antivírus segundo a gravidade das suas acções, a facilidade de infecção e o nível de disseminação mundial:

- **Baixo risco**
  vírus que apenas efectua pequenas brincadeiras como emitir sinais sonoros ou apresentar mensagens de forma periódica. Podem também efectuar alguns danos mas neste caso apenas infectam aplicações raramente utilizadas.

- **Risco médio**
  vírus já bastante disseminado e com alguma facilidade para infectar computadores, podendo provocar a eliminação de ficheiros. A maior parte das vezes o utilizador apercebe-se que o seu computador foi infectado.

- **Alto risco**
  vírus de fácil propagação e de disseminação rápida, normalmente de origem recente e que pode provocar danos significativos no seu computador, nomeadamente eliminando todo o conteúdo do seu disco duro. Os piores vírus deste tipo são aqueles que alteram os dados de um computador sem que o utilizador se aperceba do facto.

1.4 Protecção contra os vírus: 10 recomendações

Para evitar que o seu computador seja infectado por vírus deverá seguir as seguintes recomendações:

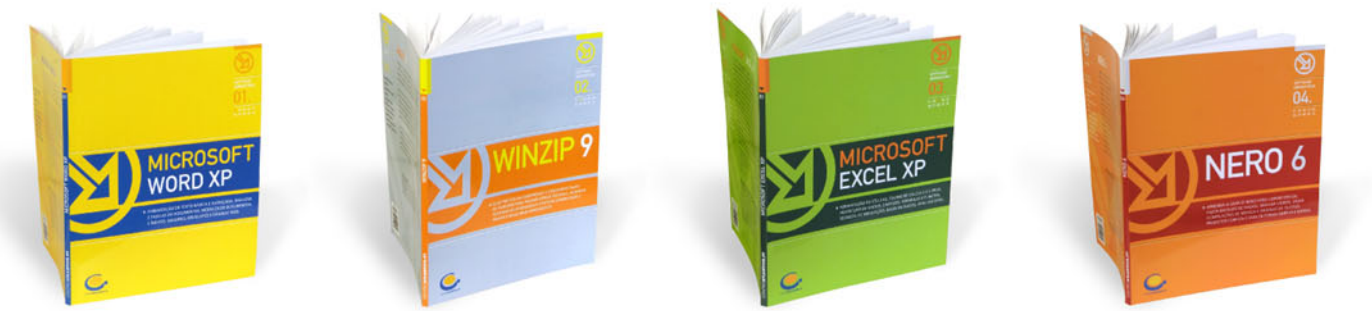
1 Instale todas as actualizações (*updates*) disponibilizadas pelo fabricante do sistema operativo e das aplicações que utiliza quotidianamente. O Windows inclui a característica de Automatic Updates para transferir automaticamente as últimas actualizações de segurança da Microsoft quando o seu computador estiver ligado à Internet. Consulte para tal o livro sobre o Windows XP, também nesta colecção. Outras actualizações obrigatórias são as que dizem respeito ao *browser* e ao software de correio-electrónico que utiliza no seu computador. Veja como fazer essas actualizações nos livros sobre o Internet Explorer 6 e o Outloook Express 6, também nesta colecção.

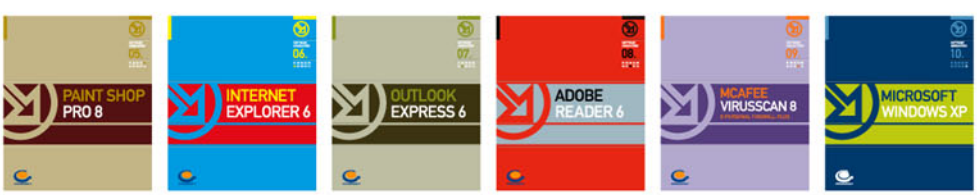
2 Instale um programa antivírus, mantenha-o actualizado e bem configurado. Cada mês são descobertos cerca de 500 vírus, por isso deverá estar sempre protegido. As actualizações do software antivírus deverão incluir não só os ficheiros com as assinaturas dos vírus (*virus signature files* ou *virus definition files*) como o motor de análise (*scanning engine*).

COLECÇÃO
SOFTWARE OBRIGATÓRIO

PARA TRABALHAR COM UM COMPUTADOR SÓ TEM QUE SABER CONTAR ATÉ 10!

10 Ferramentas informáticas fundamentais





Livros com actualização gratuita* durante 6 meses.

*A compra da caixa com os 10 livros dá direito a receber, gratuitamente, as actualizações aos livros num período de 6 meses. Válido para os cupões de actualização recebidos até Dezembro de 2004.

01. Microsoft Word XP
02. WinZip 9
03. Microsoft Excel XP
04. Nero 6
05. Paint Shop Pro 8
06. Internet Explorer 6
07. Outlook Express 6
08. Adobe Reader 6
09. McAfee VirusScan 8
10. Microsoft Windows XP

NOTA DE ENCOMENDA

PODE SER FOTOCOPIADA

TÍTULO	PREÇO LANÇAMENTO	PREÇO
☐ CAIXA COM OS 10 LIVROS DA COLECÇÃO SOFTWARE OBRIGATÓRIO	79,65 €	~~88,50 €~~

Todos os preços já incluem IVA à taxa em vigor.

SIM, desejo receber a caixa com os 10 livros sem qualquer despesa de envio.

☐ Envio cheque/Vale nº _____ à ordem do Centro Atlântico.

☐ Prefiro que debitem no meu cartão de crédito:

Número do cartão de crédito: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Cartão em nome de _____

Últimos três digitos nas costas do cartão: ☐☐☐ Validade: ☐☐☐☐ Mastercard ☐ Visa ☐ American Express ☐

Empresa _____

Nome _____

Morada _____

CP ☐☐☐☐-☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Tel. ☐☐☐☐☐☐☐☐☐

E-Mail _____ Contribuinte ☐☐☐☐☐☐☐☐☐

Sem despesas de envio. As encomendas directas ao Centro Atlântico, para Portugal, não pagam custos de portes. Envios à cobrança são onerados em 2,5 € por encomenda. Envios internacionais são onerados em 5 €.
Os dados recolhidos são processados automaticamente pelo Centro Atlântico e destinam-se à gestão do seu pedido e à apresentação de futuras propostas. O seu fornecimento é facultativo. É garantido, nos termos da Lei, o direito de acesso e de rectificação bem como de não divulgação a terceiros, devendo dirigir-se para tal ao Centro Atlântico. Se não desejar receber informações sobre os nossos produtos e serviços assinale aqui com uma cruz: ☐

CENTROATLANTICO.PT

Dirija as suas encomendas para: Centro Atlântico - Rua da Misericórdia, 76 - 1200-273 LISBOA