Versão 1.2

Muitos usuários de Windows estão com seus computadores infectados por malwares (worms, adwares, spywares, trojans ...) e só sabem disso quando o sistema operacional começa a se comportar de maneira estranha. Os sintomas disso incluem:

- janelas do Internet Explorer abrindo sozinhas
- sites desconhecidos aparecem quando se quer fazer uma busca
- o Internet Explorer tem uma nova página inicial sem que você tivesse configurado-o para isso
- programas anti-spywares deixam de funcionar (ao serem abertos, fecham-se automaticamente)
- o acesso à Internet torna-se lento sem motivo
- o Windows está mais lento do que de costume
- há um tráfego adicional na sua rede sem motivo

Ao acontecer isso, é normal o usuário xingar o Windows e a Microsoft e "rebootar o micro para ver se melhora" - e continuar irritado ao ver que não há melhora alguma depois de (inutilmente) reinicializar o computador.

Os malwares vêm embutidos em diversos de programas gratuitos na web que "seduzem" o usuários para instalá-los, infectando o computador dele sem que ele perceba.

Alguns dos conhecidos programas que fazem isso são o KaZaA, Gator, GAIN, PrecisionTime, DashBar, Date Manager, WeatherScope, WeatherCast, ClockSync, BonziBuddy, IEHelper, SnagIt, MySearch, Comet Cursor entre muitos outros.

Você pode obter uma lista com programas que contém malwares em diversos sites como este e este ...

Mas o que é **malware** ? Malware reúne toda gama de programas que realizam tarefas nocivas sem que o usuário saiba e os 7 tipos mais conhecidos são:

Spywares, que monitoram o uso do computador, podendo roubar informações como a sua lista de endereços de e-mail, por exemplo, enviando-a para spammers

Adwares, que podem mostrar banners aleatoriamente e monitorar o seu uso da Internet, podendo roubar informações relativas à navegação (sites visitados)

Trojans, programa que ao se instalado no seu computador, abre um canal de comunicação externo para que hackers possam acessar o seu computador sem o seu conhecimento

Hijackers, programas que alteram o comportamento do seu browser, fazendo com que ele acesse páginas e sites

específios sem que você tenha configurado-o para isso.

Worms, programas que têm como finalidade se propagar e infectar o maior número de computadores, fazendo com que eles automaticamente enviem milhares de e-mail, ataquem sites ou realizem tarefas específicas

Virus, programas que têm como finalidade destrutiva, infectando arquivos, partições, setores de boot ...

Keyloggers, programa que armazena tudo o que você digita no seu teclado e envia o arquivo para hackes analisarem, podendo com isso roubar senhas, logins, número de cartão de crédito ...

A solução definitiva para a eliminação dos malwares é um conjunto de três tarefas:

1. Desinstalação dos programas que contém malwares (quando isso é possível, pois muitos destes programas não têm desinstaladores)

2. Utilização de programas específicos para a detecção e eliminação dos malwares

3. Modificação do Windows para minimizar a reinstalação dos mesmos

Como estas tarefa não são simples de serem feitas, eu criei este guia que mostra como fazer isso de maneira simples e direta, além de ajudá-lo a evitar que novos malwares se instalem em seu computador.

Este guia também ajudará você a descobrir se o seu micro está infectado com worms (que enviam milhares de mensagens de e-mail sem que você saiba), algo que pode passar despercebido pelo usuário, pois como não há sinal algum visível de problema no Windows, ele pode concluir erroneamente que o micro dele não está infectado.

Para manter você atualizado em relação aos malwares, informando novidades sobre eles e como removê-los, criamos uma **área no Fórum do BABOO** aonde você pode postar dúvidas e problemas que você está tendo com malwares para que a comunidade do Fórum ajude-o, bem como um **tópico específico sobre este guia**, aonde você pode obter informações adicionais acompanhar todas as novidades**.**

É importante que você perca alguma horas seguindo cada passo deste Guia pois isso poderá economizar muita dor-de-cabeça e perda de tempo caso o seu computador esteja infectado e você ainda não tenha eliminado os malwares deles. Arme-se de paciência e bom-humor pois no final terá valido a pena !

Este guia tem 20 passos que ensinam você como eliminar os malwares e impedir que eles voltem. Os passos 1 a 11 mostram como identificar e eliminar todos os malwares do seu computador e os passos 12 a 20 mostram como evitar que eles reapareçam.

Este Guia está dividido em 20 passos:

Este guia sugere o uso de diversos programas gratuitos que podem ser obtidos no site do desenvolvedor dos mesmos. Para facilitar o seu trabalho, disponibilizamos dois links no BABOO contendo arquivos com estes programas:

Arquivo sem o Zone Alarm
Ad-Aware SE 1.03, AdwareAway 2.23, Autoruns 5.0, BHODemon 2.0.0.18, CWShredder 1.59.1, Spybot 1.3
Tamanho: 9,6 Mb
Indicado para quem já tem um firewall instalado ou para quem usa Windows XP

Arquivo com o Zone Alarm
Ad-Aware SE 1.03, AdwareAway 2.23, Autoruns 5.0, BHODemon 2.0.0.18, CWShredder 1.59.1, Spybot 1.3, ZoneAlarm 5.1.011
Tamanho: 15,1 Mb
Indicado para quem não tem firewall instalado ou para quem não usa Windows XP

1 Como saber se o seu computador está infectado ?

Embora no decorrer deste guia você saberá em detalhes como identificar e eliminar malwares, uma das maneiras mais rápidas de se fazer isso é **visualizar os programas que são executados quando o Windows é carregado** pois desta maneira pode-se saber quais programas desconhecidos estão listados ali - e que usualmente são malwares.

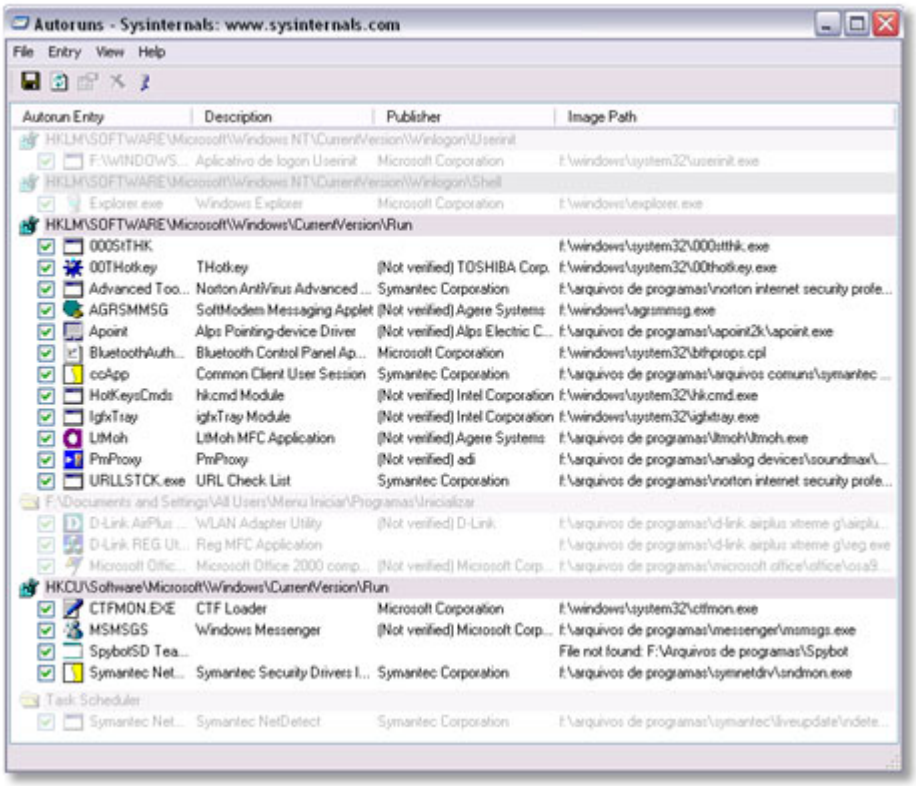
Para fazer isso, faça o download do pequeno arquivo Autoruns 5.0: ele é gratuito, tem apenas 140 Kb e não necessita de instalação. Ao ser executado, abre-se uma janela listando os arquivos que são carregados juntamente com o Windows, durante a inicialização deste.

(outra maneira de ver os arquivos carregados na inicialização do Windows é utilizar o utilitário MSCONFIG que vem no Windows, embora ele seja mais restrito e menos detalhado do que o Autoruns)

Para saber se o seu computador tem algum malware, execute o Autoruns e observe a lista de programas existentes logo abaixo das linhas

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run e
HKCU\Software\Microsoft\Windows\CurrentVersion\Run:

Veja a imagem:



Verifique se há algum arquivo suspeito sendo carregado, seguindo estas três dicas:

1. Arquivos localizados na pasta Temp ou Temporary Internet Files (veja a localização dos arquivos na coluna Image Path)

2. Arquivos com colchetes: amovoce[1].exe, por exemplo

3. Arquivos com extensão .dll

Se houverem arquivos com as características acima, é recomendável você clicar no quadrado à esquerda dele para desabilitá-lo e reiniciar o Windows após isso.

Exemplos de arquivos listados na coluna Image Path que indicam ser malwares:

c:\windows\hello.exe
c:\windows\temp\mysearch.exe
c:\Documents and Settings\Joao\Local Settings\Temporary Internet Files\hi.exe
c:\windows\temp\drv32.exe
c:\windows\avserve2.exe

2 Verifique o arquivo HOSTS

O Windows mantém um arquivo chamado HOSTS que contém uma lista de IPs e nomes de domínios que visa agilizar ou redirecionar o acesso a alguns sites.

Alguns malwares modificam o arquivo HOSTS para que o computador não consiga acessar sites de atualização de antivirus, Windows Updates e outros - portanto o primeiro passo é verificarmos se o seu arquivo HOSTS está íntegro. No Windows XP, o arquivo HOSTS (que não tem extensão) encontra-se em *\Windows\System32\Drivers\ETC* e no Windows 9x/Me ele está em *\Windows.*

Vá até a pasta aonde o arquivo HOSTS está localizado, clique nele com o botão da direita do mouse e escolha a opção *Abrir*. Por ser um arquivo texto, o Windows poderá abri-lo com o Bloco de Notas.

O arquivo HOSTS contém algumas linhas que começam com o caractere # e uma ou mais linhas com números e palavras. Para certificar que o seu arquivo HOSTS está íntegro, usualmente ele deve conter apenas uma linha:

127.0.0.1 localhost

Se houver mais linhas ali (que não têm o símbolo # como primeiro caractere), é recomendável que você apague todas elas.

Linhas como as listadas abaixo mostram claramente que o seu arquivo HOSTS está danificado por algum malware (pois os sites listados ali não poderão ser acessados) e por isso essas linhas devem ser imediatamente apagadas:

127.0.0.1 download.mcafee.com
127.0.0.1 f-secure.com
127.0.0.1 kaspersky.com

127.0.0.1 liveupdate.symantec.com
127.0.0.1 liveupdate.symanteclive update.com
127.0.0.1 mcafee.com
127.0.0.1 symantec.com
127.0.0.1 trendmicro.com
127.0.0.1 www.grisoft.com
127.0.0.1 www.kaspersky.com
127.0.0.1 www.mcafee.com
127.0.0.1 www.sophos.com
127.0.0.1 www.symantec.com

Após apagar todas as linhas adicionais, salve o seu arquivo HOSTS.

3

Habilite seu firewall
Tenha certeza que o Internet Connection Firewall (do Windows XP com SP1 ou sem nenhum Service Pack instalado), o Windows Firewall (do Windows XP SP2) ou qualquer firewall que você utilize, está ativado e funcionando corretamente.

Para saber se o seu firewall está funcionando, siga estes passos simples:

1. Acesse o site do **Gibson Research** **(GRC)**
2. Clique em Shields UP!
3. Clique no botão Proceed
4. Clique na opção Common Ports
5. Após alguns segundos, aparecerá o resultado

O ideal é que as principais portas TCP/IP do seu computador estejam fechadas (Closed) ou escondidas (Stealth), como mostrado na imagem abaixo.

Se o resultado do seu computador mostrar que as portas 135, 139 e 445 estão abertas, é possível que o seu computador esteja infectado com algum malware.

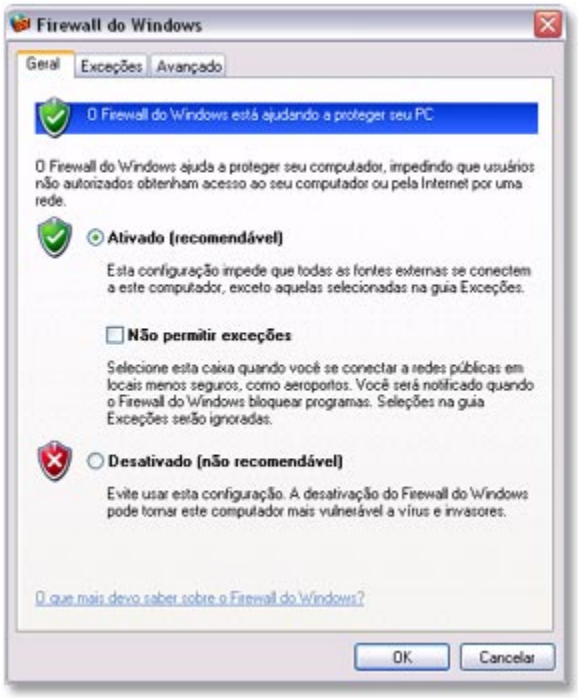
Se o computador que você fizer o teste não está fisicamente conectado à Internet, ou seja, há outro computador que

está disponibilizando a conexão da web para você, o teste de segurança será realizado naquele computador - e não no seu. Isso não muda em nada a validade do teste do GRC pois o importante é que o computador que está fisicamente conectado à Internet esteja protegido, pois é por ali que hackers tentarão invadir o computador ou a rede local.

O firewall impede que hackers invadam o seu computador e também impede que alguns bugs do Windows XP possam ser explorados remotamente (como a vulnerabilidade que informava que o Windows seria desligado em um minuto). Para hablitar o firewall no Windows XP, faça o seguinte:

No Windows XP com SP1 ou não: vá em *Iniciar* > *Painel de Controle* > *Conexões da Internet* > dê um duplo-clique na sua conexão > *Propriedades* > *Avançado* > clique na opção de Firewall de conexão com a Internet ("*Proteger o computador e a rede limitando ...*") e clique em *OK*

No Windows XP com SP2: vá em *Iniciar* > *Painel de Controle* > *Firewall do Windows* > certifique que a opção *Ativado* está habilitada



Se você não utiliza o Windows XP, você deve utilizar um firewall de terceiros, como por exemplo o **ZoneAlarm**, que é um firewall gratuito muito eficiente.

Outra ótima opção de firewall é o Norton Personal Firewall (ou o Norton Internet Security, pacote que inclui o Norton Antivirus) da Symantec.

4

Atualize o seu antivirus
Além de confirmar se o seu antivirus está atualizado (faça isso atualizando-o via web ou verificando no site da empresa que o desenvolveu), você deve fazer uma verificação completa dos seus discos rígidos.

O Service Pack 2 do Windows XP inclui a Central de Segurança, que informa se o seu antivirus está atualizado ou não.

Uma dica importante é que você deve configurar o seu antivirus para **proteção máxima** para que todos arquivos suspeitos possam ser interceptados, pois a maioria dos antivirus vêm configurados com proteção média e você deve verificar e alterar isso.

No Norton Antivirus, por exemplo, você deve clicar em *Opções* > clicar em *Auto-Protect* > *Bloodhound* > habilitar a opção "*Nível mais alto de proteção*". O mesmo deve ser feito na opção *Verificação Manual* > *Bloodhound*.

Um detalhe importante sobre o AVG: muitos usuários usam o antivirus AVG 6.0 pois ele é gratuito - e infelizmente esse antivirus é ruim, dando a falsa impressão ao usuário que ele está sem vírus, quando na verdade o micro pode estar infectado sem que este antivirus seja capaz de detectar isso.

Por isso, na minha opinião você deve fugir do AVG: desinstale-o e instale algum antivirus decente como o Norton Antivirus, McAfee, NOD32, Panda ou outros pois com estes o seu computador com certeza estará muito mais protegido.

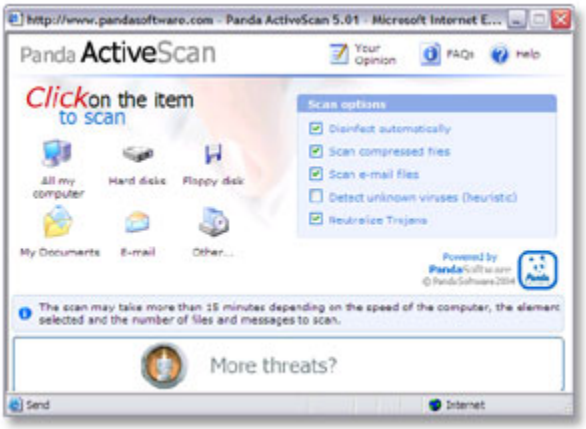
É muito importante você fazer a verificação completa dos seus discos rígidos (mesmo que isso demore algumas horas) antes da próxima etapa pois de nada adianta atualizar o seu Windows se ele estiver infectado sem que você saiba !

5

Execute o scan online da Panda Software

Embora o antivirus da Panda Software não esteja entre os mais utilizados, a verificação online via web da empresa mostra ser surpreendentemente eficiente contra diversos tipos de vírus e worms.

Para acessar o Panda ActiveScan, clique **aqui**. Ao clicar no botão *Scan your PC,* você será redirecionado para outra página aonde você deve clicar no botão *Next*. Depois basta preencher um endereço de e-mail e clicar em *Send*. Por fim, indique a sua localização e clique em *Start*.



Depois disso a página enviará um arquivo que deve ser executado para que a análise online possa ser realizada.

Você poderá escolher o que será analisado e sugiro que você escolha *Meu Computador* para que todos os drives do seu computador sejam analisados.

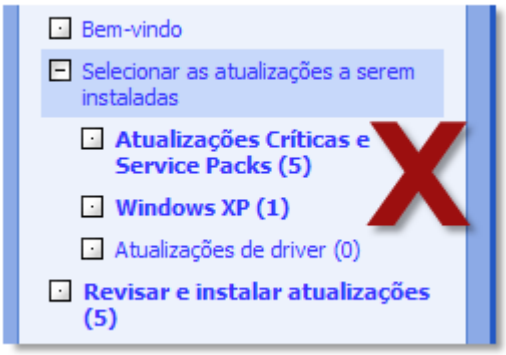
A análise demora alguns minutos e no final os arquivos infectados são eliminados.

Também estão disponíveis outras verificações online de fabricantes de antivirus, como **Symantec**, **McAfee**, **BitDefender** e **Trend Micro**.

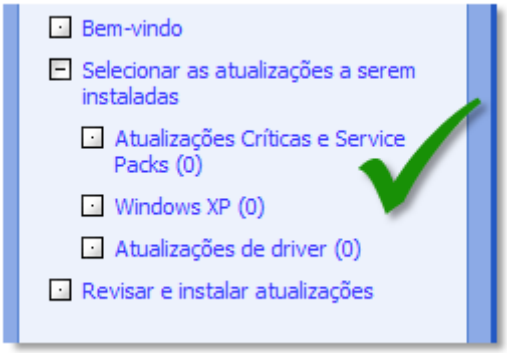
6

Instale todas as Atualizações Críticas e Service Packs existentes no Windows Update.
Ao acessar o **Windows Update** e instalar todas as atualizações críticas listadas ali, o seu Windows eliminará diversas vulnerabilidades que são aproveitadas por vírus, worms e outros malwares.

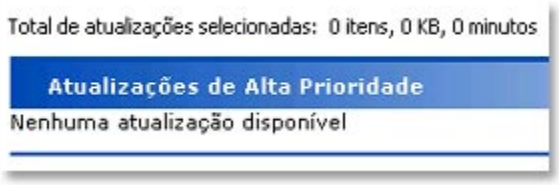
É importante você saber que toda segunda terça-feira de cada mês (10/Ago/04, 14/Set/04, 12/Out/04 ...), a Microsoft disponibiliza um pacote de atualização para o Windows e seus componentes (Internet Explorer, Outlook Express, Windows Media Player ...), facilitando a previsão de novos updates - embora em casos especiais possam haver updates importantes disponibilizados em outras datas.



É importante que você instale TODAS as Atualizações Críticas e Service Packs existentes para garantir que o seu Windows esteja atualizado. Usuários com conexão a modem podem **pedir gratuitamente à Microsoft o envio de um CD com o Service Pack** caso queira evitar obtê-lo via Internet.



O maior update (excluindo-se Service Packs) é o .NET Framework e embora ele seja importante para uso de aplicações desenvolvidas para a plataforma .NET, você não precisa instalá-lo sob o ponto de vista de segurança do seu computador. O Windows Update 5.0 é a versão atual do Windows Update e para os usuários do Windows XP, ele provê diversas novidades, incluindo arquivos menores para download e uso limitado de banda para não atrapalhar a navegação.



Windows Update 5.0 indicando que não há nenhuma atualização disponível

O Windows Update permite que você salve em seu computador os arquivos obtidos ali; desta maneira você pode instalá-lo em outros computadores sem a necessidade de obtê-los novamente via Internet.

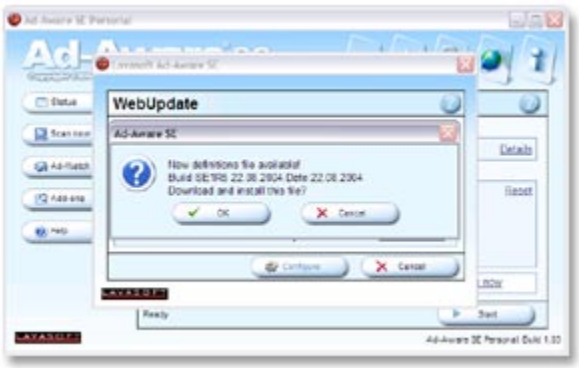
Para fazer isso, clique na opção *Opções do administrador* (à esquerda) e clique no link *Catálogo do Windows Update* (à esquerda, dentro do parágrafo sobre Atualizar vários sistemas operacionais)
Embora existam sites que façam gratuitamente uma varredura online do computador do usuário para detectar malwares, como o **PestScan** da PestPatrol, é recomendável você fazer isso através de software gratuitos, que são mais completos e melhor indicados para esta tarefa:

7.

Instale e execute o Ad-Aware SE (programa gratuito)
O Ad-Aware SE Personal Edition é um programa gratuito e muito eficiente para a eliminação de adwares (programas que mostram banners de anunciantes). Ele pode ser obtido no site da Lavasoft USA.

A instalação do Ad-Aware é bastante elementar e não há opção para configurações específicas na instalação. Após a instalação do produto, aparecerá na última tela três opções: *Perform a full system scan now*, *Update definition file now* e *Open the help file now*. Clique apenas na segunda opção (*Update definition file now*) e clique no botão Finish.

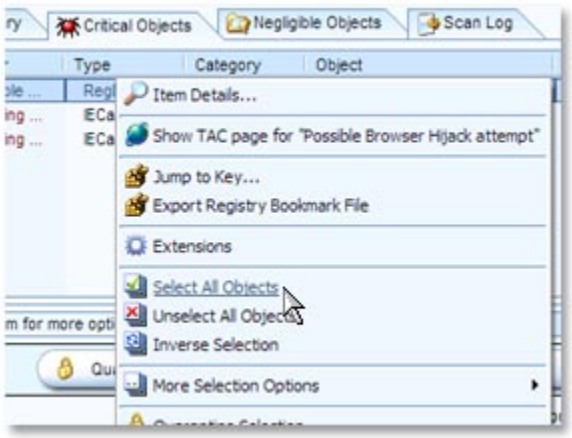
O programa será carregado e você deve clicar na opção *Check for updates now* e depois no botão *Connect.* Ao aparecer a mensagem indicando que há updates disponíveis para download (como mostrado na imagem abaixo), clique no botão OK para instalá-los. Quando finalizar a instalação, clique no botão *Finish*.



Agora que o Ad-aware está atualizado, você deve utilizá-lo para fazer uma varredura no seu computador. Para isso, clique no botão *Status* (o botão superior à esquerda) e em seguida no botão *Start*. Selecione a opção *Perform full system scan* (segunda opção) e clique em Next. Aguarde a finalização da varredura.

Ao finalizar a verificação, clique no botão *Next* e você verá a lista de arquivos encontrados. Para obter informações sobre cada um dos arquivos encontrados, basta dar um duplo-clique no nome e você terá uma descrição completa do mesmo.
Para eliminar todos os arquivos (o que é altamente recomendável), clique com o botão da direita do mouse em

qualquer lugar da janela > escolha a opção *Select all objects* (imagem abaixo) e clique no botão *Next*. Clique em OK para eliminar os arquivos encontrados.



É importante que você saiba que alguns programas que utilizam adwares não funcionam mais caso ele seja eliminado (como o KaZaA) e que muitos dos arquivos mostrados pelo Ad-Aware são cookies (que são listados com a palavra "Tracking" na coluna Vendor), que são arquivos comumente utilizados por alguns sites para controle de acesso e que são automaticamente recriados quando você acessa novamente o site.

O mais importante no Ad-Aware é que ele localiza e elimina adwares perigosos, contidos em arquivos e linhas no Registro do Windows, pois comparados com os malwares existentes, os cookies não representam perigo de segurança para o internauta (embora algumas empresas de marketing utilizem-nos para rastrear os sites navegados pelo internauta).

Após realizar essa varredura com a opção *Perform full system scan*, você pode utilizar a opção recomendada (*Perform smart system scan*) nas próximas vezes (item 19).

8

Instale e rode o Spybot (programa gratuito)
O Spybot (cuja versão mais recente é a 1.3) é provavelmente o melhor programa para eliminar spywares.

Ao instalá-lo, tenha certeza de habilitar a opção para instalar o SDHelper e principalmente o TeaTimer, um pequeno aplicativo que monitora o Registro, evitando que spywares façam modificações ali sem que o usuário saiba.

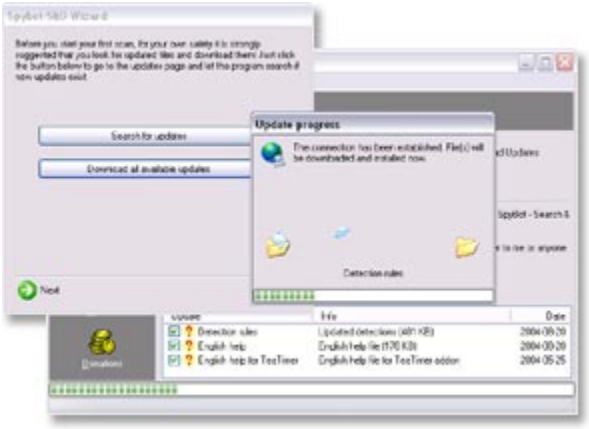
Quando o TeaTimer está rodando, é comum aparecer algumas mensagens dele quando é realizada atualização do Windows (item 6 acima) pois estas usualmente fazem modificações no Registro do Windows: isso é normal e você deve aceitar as modificações.

Após finalizar a instalação do Spybot e executá-lo, o programa sugere realizar três importantes tarefas que ajudam na proteção do seu computador e é ALTAMENTE recomendável que você aceite-as. São elas:

1. Create Registry Backup, que fará um backup do Registro do Windows. Ao clicar no botão *Create registry backup*, a opção Next (na parte inferior da janela, ao lado da seta verde) ficará cinza até a finalização do backup (que pode demorar alguns minutos)

2. Search for Updates e Download all available updates, que procurará atualizações para o programa e as instalará, caso existam.

Essa etapa é importantíssima pois permite que o Spybot atualize-se, permitindo a identificação e remoção de novos malwares que possam estar instalados no seu computador.



Após a finalização do processo (quando a janela *Update progress* desaparecer e a lista de atualizações tiver o símbolo ✓), clique em *Next*.

3. Immunize this system, que imunizará o computador contra diversos malwares, evitando que eles sejam instalados no computador. Ao clicar em *Next*, aparecerá na janela o número de programas ruins (malwares) bloqueados que não poderão ser instalados. Clique então em *Next* e no botão inferior *Start using the program*.

Rodando o Spybot
Agora que o programa está instalado e atualizado, você deve executá-lo para que ele detecte spywares instalados no seu computador. Para isso, clique na opção *Search & Destroy* (primeiro ícone superior na janela à esquerda) e em seguida em *Check for problems*.

Após alguns minutos (sendo que às vezes o programa parece estar travado, mas não está), o programa mostrará uma lista de arquivos que envolvem malwares e também cookies de empresas de banners (que podem fazer com que essas empresas monitorem a sua navegação nos sites gerenciados por elas).

Um detalhe interessante é o **DSO Exploit**, usualmente detectado pelo Spybot, mas que na realidade são chaves do registro relativas a Zonas do Internet Explorer e que não oferecem perigo algum.

Para eliminar todos os arquivos encontrados, clique na opção *Fix selected problems* e os arquivos serão apagados após você confirmar que deseja removê-los. Se você utiliza o Windows XP, é criado um Ponto de Restauração por questão de segurança.

Quando o Spybot não consegue eliminar o arquivo (pois ele está ativo na memória, por exemplo), ele informa-o disso e pergunta se você deseja que esses arquivos sejam eliminados na próxima vez que o computador for ligado. É importante que você aceite isso e reinicie o computador o mais breve possível, pois dessa maneira o Spybot será executado no início do Windows e os arquivos poderão ser (enfim) eliminados.

Opção Immunize
Um detalhe muito útil para fazer depois do Spybot confirmar que você não tem nenhum arquivo suspeito no seu micro é clicar a opção Immunize para ter certeza que o seu computador ficará imune a alguns malwares.

Tenha certeza que a segunda opção do Imunnize ("*Enable permanent blocking of bad addresses in Internet Explorer*") esteja clicado e a opção "Block all pages silently" selecionada. Para ter certeza que o seu sistema está razoavelmente imune, clique no botão superior *Immunize*.

TeaTimer
Usuários mais atentos devem ter notado um novo ícone no tray (ao lado do relógio): é o TeaTimer, um aplicativo que monitora algumas chaves do Registro do Windows, avisando o usuário sempre que algum programa tentar modificá-las.

O TeaTimer é muito útil pois permite manter o computador mais seguro, informando quando algum programa tenta modificar o Registro - mesmo programas conhecidos e importantes, como durante a Atualização Automática do Windows, atualizações do antivirus, ou quando o usuário instalar algum programa novo.

Antes de instalar um Service Pack, é recomendável que você desabilite o TeaTimer

Quando algum programa tentar alterar o Registro do Windows ou o Internet Explorer (ao instalar a barra da MSN ou do Google, por exemplo), o TeaTimer permite que você permita que a mudança seja feita (*Allow change*) ou que ela seja recusada (*Deny change*). Além disso há a opção *Remember this decision* que permite que o TeaTimer relembre a opção que você definiu e aplique-a novamente, evitando que a janela apareça a todo instante.

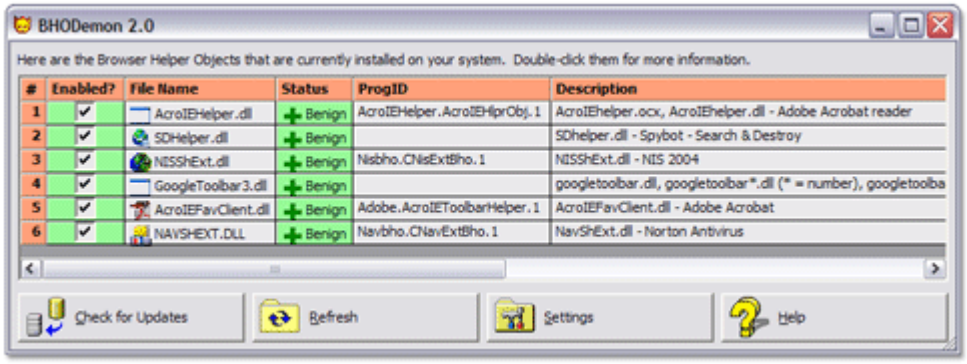
O Spybot é um programa bastante poderoso, permitindo a verificação de mais opções além de spywares. Além do programa poder ser configurado para idioma português brasileiro (menu *Language* > *Brasil*), você pode habilitar a opção Avançada (menu *Mode* > *Advanced Mode*), o que trará muitas outras opções. Exemplo: clique na barra Tools (Ferramentas) e você poderá alterar a configuração de BHOs, ActiveX, arquivo HOSTS, entre outras opções.

Instale e execute o BHO Demon (programa gratuito)
Se você não utiliza o Service Pack 2 do Windows XP, então você deve fazer o download do BHO Demon, que permitirá que você saiba quais Browser Helper Objects (BHOs) estão habilitados no Internet Explorer (IE). O programa pode ser obtido aqui ou aqui.

Alguns programas instalam extensões no IE que facilitam o uso dos mesmos (como o Adobe Reader, que integra a visualização de arquivos .PDF no IE, alguns gerenciadores de download, antivirus entre outros), mas isso também permite que spywares instalem ali o que quiserem. Esses programas que instalam extensões (ou integram-se ao IE) são denominados BHO (Browser Helper Objects).

Muitos malwares utilizam essa técnica: versões antigas do Go!Zilla (gerenciador de downloads), por exemplo, instalavam um BHO que monitorava o uso do IE. A maneira mais simples de saber se o seu IE tem algum BHO spyware que não foi detectado pelo Ad-aware e Spybot é visualizando a lista de BHOs - e o ótimo BHO Demon faz exatamente isso, avisando-o se há algum BHO suspeito.

Ao instalar e executar o BHO Demo, o primeiro passo que você deve realizar é clicar no botão "*Check for Updates*" e clicar em "*Check NOW for a New Version of BHODemon*". Clique em OK e instale todas as atualizações existentes. Agora é hora de você eliminar os BHO suspeitos:



Na imagem acima você tem a lista de BHO (são 6 ao todo), aonde eles são tidos como Benignos (Benign, escrito em verde). Para obter mais informação sobre um determinado BHO, dê um duplo-clique nele e abrirá uma janela mostrando detalhes do arquivo.

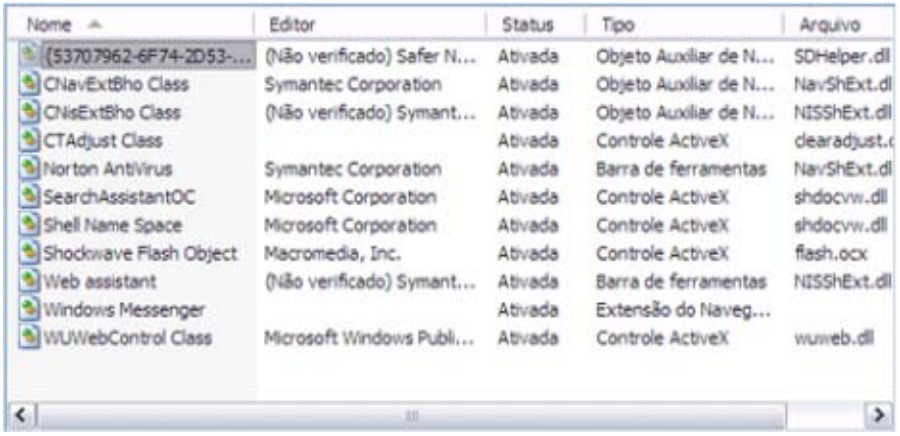
No nosso caso, os BHO instalados são estes:
1. AcroIEHelper = Adobe Reader
2. SDHelper.dll = aplicativo do Spybot
3. NISShExt.dll = Norton Internet Security
4. GoogleToolbar3.dll = barra do Google
5. NAVSHEXT.dll = Norton Antivirus

Caso exista algum BHO suspeito no seu micro, você pode desativá-lo clicando no símbolo correspondente que aparece na coluna Enabled?. Qualquer programa que você não conheça pode ser um malware e é recomendável que você desabilite-o.

Usuários do Service Pack 2 do Windows XP
Usuários do Service Pack 2 do Windows XP não precisam do BHO Demon pois o IE vêm com uma função similar: o Gerenciador de Complementos, que está na opção *Ferramentas* > *Opções da Internet* > aba *Programas* > botão *Gerenciar Complementos*.

O Gerenciador de Complementos lista os BHO instalados no seu computador, permitindo que você desative-os a qualquer instante.

Embora isso seja suficiente para impedir de algum BHO indesejável funcionar, o uso do BHO Demon continue sendo recomendável por fornecer muito mais detalhes sobre os BHOs instalados.



Na imagem acima, pode-se ver diversos aplicativos BHO conhecidos que são executados juntamente com o Internet Explorer, como o Norton Antivirus, Shockwave Flash e Windows Messenger - e outros nem tão reconhecidos, como o SDHelper (aplicativo do Spybot) e CTAdjust Class (ActiveX que permite a configuração do ClearType).

Caso você desconfie de um deles, desabilite-o clicando na opção Desativar (que não está mostrada na imagem acima) e volte a utilizar o browser para verificar se ele continua funcionando corretamente. Você poderá fazê-lo voltar a funcionar bastando clicar no nome dele e selecionar a opção Ativar.

10

Instale e execute o CWShredder (programa gratuito)
O CWShredder elimina muitos trojans conhecidos e embora ele tenha sido descontinuado pelo desenvolvedor, ele continua resolvendo diversos problemas comuns que muitos internautas têm quando o seu browser parece ter "vida própria". O CWShredder pode ser obtido aqui.

O CWShredder elimina diversos problemas como redirecionamento de URL, mudanças na página inicial, janelas pop-up e outras ações características de hijackers.

O seu uso é bastante simples: você deve fechar todas as janelas do Internet Explorer e clicar a opção *Next*.

O programa verificará a existência de diversos malwares (embora muitos recentes não estão na lista) e eliminará aqueles que forem detectados.

O criador do CWShredder também criou o HiJackThis! um ótimo programa que permite visualizar os arquivos que são carregados na inicialização do Windows, entre outras informações úteis para quem tem conhecimento para lidar com elas. O HiJackThis! pode ser obtido aqui.

11

Novos spywares e hijackers ? Adware Away neles ! (programa trial)
O Adware Away é a mais nova arma contra malwares, que completa a tarefa do Ad-Aware e do Spybot, procurando e eliminando malwares. Você pode obter o Adware Away no site da empresa que o desenvolveu, sendo que a versão atual é a 2.2. Ele permite o uso gratuito por 5 dias.

O grande diferencial entre o Adware Away e os demais programas de eliminação de spyware é que o Adware Away tem ferramentas para eliminação de determinados hijackers (programas que alteram o Internet Explorer fazendo com que o internauta seja redirecionado para sites sem o seu consentimento) que usualmente só conseguem ser removidos "à mão" após a realização de diversos passos para isso.

Entre alguns hijackers complexos que são eliminados pelo Adware Away estão o **about:blank** (em que aparece na barra de endereços do IE "about:blank" mas o browser carrega várias páginas), o **res://dll** (a barra de endereços contém res://[nome].dll/index.html#) e o **SSearch.biz** (aonde a barra de endereços sempre contém algo como "ssearch.biz?wmid=".

A cada nova versão, o Adware Away adiciona a eliminação de novos spywares e por isso ele torna-se uma excelente ferramenta contra os malwares.

O ponto negativo do programa é que na versão atual, a varredura de spywares detecta um arquivo importante do sistema operacional (userinit.exe) como um arquivo "suspeito", o que poderia causar problemas caso o usuário decidisse apagá-lo - e portanto só recomendo este programa por causa da (excelente) varredura e eliminação de hijackers.

Usando o Adware Away

A instalação do programa é bastante simples e a primeira tarefa a ser realizada é a atualização do programa, que deve ser feita clicando-se na opção *Online Update* (à esquerda, na parte inferior). Se houver alguma atualização, instale-a imediatamente. Para iniciar a varredura, clique na opção *Scan*. O Adware Away permite que você faça uma varredura para achar e eliminar hijackers.

Para isso, clique na opção Hijacker Away (à esquerda, dentro do módulo Specialized Remover) e logo em seguida clique no terceiro ícone na parte inferior da janela, conforme ilustrado na imagem abaixo.

Caso algum hijacker for encontrado, você deve verificar qual o nome dele na janela de resultados, clicar no ícone correspondente na parte superior da janela e, por fim, clicar no último ícone da lista, que eliminará o malware.

Exemplo prático: vamos supor que o seu computador esteja infectado com o hijacker MyWebSearch mas você não sabe disso. Você deve seguir estes passos:

1. Clique na opção Hijacker Away e no terceiro ícone (mostrado na imagem acima) para fazer uma varredura à procura de qualquer hijacker

2. Aparecerá na lista Totally Found: [1] Malware Objects!, indicando que foi encontrado um malware no seu computador !

3. Para saber qual é esse malware, você deve subir a lista e localizá-lo: neste caso, aparecerá Found [1] MyWebSearch Hijacker, indicando que o seu computador está infectado com o MyWebSearch.

4. Na lista de ícones da parte superior, você deve clicar no ícone MyWebSearch Hijacker, indicando que este é o malware que você pretende eliminar

5. Agora você deve clicar no último botão (o último à direita), que eliminará o malware escolhido (MyWebSearch) do seu computador.

Um detalhe importante é que além de você clicar em Hijacker Away, procurando por **Hijackers**, você também deve fazer a varredura de **Adwares** (clicando em Adware Away), **Spywares** (clicando em Spyware Away) e **Trojans e Worms** (clicando em Trojan & Worm Away), clicando o terceiro ícone de cada um deles para certificar-se que o seu computador não está infectado com nenhum malware listado.

É importante que você saiba que o Adware Aware identifica algumas chaves no Registro (Use FormSuggest, FormSuggest Passwords, FormSuggest PW Ask e AutoSuggest, por exemplo) como Backdoor Berbew, quando na verdade essas chaves são usadas pelo IE para armazenar logins e senhas (embora também sejam utilizadas por trojans caso eles existam no computador).

Ao seguir todos os passos acima, agora o seu computador deve estar livre da imensa maioria dos malwares - portanto agora é hora de nos preocuparmos em evitar e impedir que eles voltem. Para impedir a volta de malwares, você deve seguir os próximos passos:

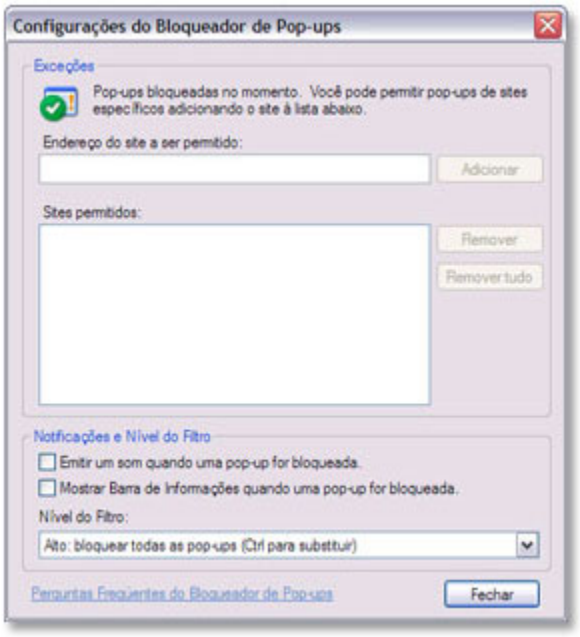
12

Utilizar um bloqueador de janelas pop-up

Isso parece ser algo simples - e realmente é: quanto menos ofertas de produtos gratuitos e milagrosos você estiver exposto, melhor, pois você evitará em cair na tentação de instalá-los e com isso colocar novos malwares no seu computador.

Embora você possa utilizar programas específicos para isso, como a barra de ferramentas da MSN ou do Google, o ideal é você utilizar o Service Pack 2 do Windows XP, que contém um bloqueador de janelas pop-up que é muito mais eficiente do que qualquer barra de ferramentas. Isso acontece pois alguns sites estão modificando o seu código-fonte para burlar (com relativo sucesso) os bloqueadores de janelas pop-up das barras de ferramentas disponíveis no mercado - mas essas modificações são inócuas quando se utiliza o bloqueador de pop-ups do próprio Internet Explorer.

Para bloquear as janelas pop-up no Internet Explorer do Service Pack 2 do Windows XP: entre no IE > clique no menu *Ferramentas* > *Bloqueador de Pop-ups* > *Configurações do Bloqueador de Pop-ups*. Desmarque as opções *Emitir um som quando uma pop-up for bloqueada* e *Mostrar Barra de Informações quando uma pop-up for bloqueada* pois isso fará com que você navegue sem ser incomodado a todo instante com informações relativas ao bloqueio de janelas pop-ups .



O *Nível do Filtro* deve ficar em Médio pois ao configurá-lo para Alto, isso impedirá a abertura de qualquer nova janela (mesmo quando você clica em links), obrigando o usuário a manter pressionada a tecla CTRL para acessar os links clicados.

13

Bloquear a instalação aleatória de ActiveX

Essa é outra medida bastante eficaz de evitar novos malwares: o bloqueio da instalação aleatória de ActiveX no seu computador, aonde cada site tenta instalar seu próprio ActiveX, fazendo com que o usuário não tenha segurança alguma ao navegar.

O bloqueio de ActiveX é feito de três maneiras:

1. Utilizando-se o Service Pack 2 do Windows XP, que automaticamente bloqueia a instalação de scripts ActiveX e só instala-os caso o usuário decida fazer isso (sendo que você pode ver os scripts ActiveX instalados acessando a opção de *Gerenciamento de Complementos* descrita no item 9 acima).

2. Configurando-se as opções "*Inicializar e executar scripts de controles ActiveX não marcados como seguros*" e "*Fazer o download de controles ActiveX não assinados*" para *Desativada* no IE. Para isso, clique no menu *Ferramentas* > *Opções da Internet* > aba *Segurança* > clique na zona *Internet* > botão *Nível Personalizado* > *Plug-ins e controles ActiveX*

3. Utilizando programas de terceiros, como o TeaTimer do Spybot (item 6 acima) e o SpywareBlaster

Há outras soluções curiosas que impedem a instalação de scripts ActiveX que são reconhecidamente spywares: o site Spyware-Guide, por exemplo, disponibiliza para download um arquivo .reg que adiciona no Registro do Windows uma lista contendo diversos scripts ActiveX que estão impedidos de serem instalados para evitar que o computador seja infectado.

14

Impedir que programas modifiquem determinadas chaves do Registro

Essa é com certeza a medida mais complexa e eficaz contra a instalação de malwares pois permite que você bloqueie a modificação de determinadas chaves no Registro do Windows, aonde ficam armazenadas as informações necessárias para que os malwares fiquem ativos sempre que o Windows for carregado - algo que na prática é o que mantém o computador sempre infectado.

Ao seguir todos os passos anteriores, você praticamente garantiu que o seu computador está limpo e isento de malwares - portanto é uma ótima hora para "fecharmos as portas" no Registro, impedindo que novos malwares infectem o seu computador.

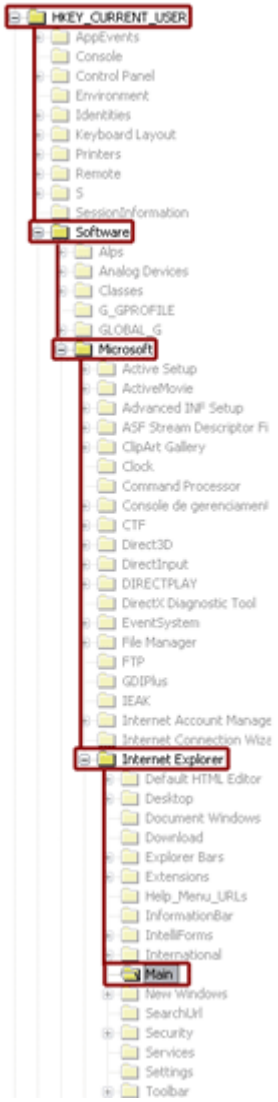
Bloqueando essas chaves do Registro fará com que o malware não possa salvar nenhuma informação ali, impedindo que ele seja executado quando o Windows for carregado, resultando no bloqueio do funcionamento do malware. A grande vantagem desta dica é que este bloqueio impede que **qualquer malware** (incluindo os que virão no futuro) seja carregado no Windows, dando uma segurança muito maior ao usuário.

A única desvantagem dessa dica é que no caso em que você precisar adicionar um novo programa que seja executado no carregamento do Windows (incluindo alguns drivers de periféricos), você deverá modificar as chaves ANTES de instalar o programa ou driver para que estes tenham permissão para fazerem isso. Após a finalização da instalação, deve-se modificar novamente as chaves do Registro visando mantê-las bloqueadas contra qualquer modificação.

Para facilitar o trabalho do usuário, estamos desenvolvendo um aplicativo em .NET que fará as modificações no Registro de maneira automática e pretendemos disponibilizá-lo para download no início de Set/04.

Esta dica exige o uso do Windows NT, Windows 2000, Windows XP Professional ou Windows 2003 com partição NTFS no drive aonde o Windows está instalado, não estando disponível para Windows 9x/Me, Windows XP Home Edition, nem para qualquer versão do Windows instalado sob partição FAT32. Para você saber qual é a partição do seu drive, vá em *Meu Computador* > Clique com o botão da direita do mouse sobre a partição aonde o Windows está instalado (usualmente C:) > *Propriedades* e veja em *Sistema de arquivos* qual é o tipo de partição (FAT ou NTFS)

Alterando as permissões de algumas chaves do Registro do Windows
Ao infectar um computador e fazer com que este continue infectado após o usuário desligar o Windows, os malwares costumam utilizar sempre a mesma técnica: carregar um arquivo infectado na inicialização do Windows.



Isso é feito de uma maneira bastante simples e eficaz pois o Windows não impede que se adicione qualquer arquivo à lista de arquivos carregados na sua inicialização - e é justamente aí que iremos intervir: vamos impedir que novos arquivos possam ser adicionados à lista atual.

É importante notar que após alterar a permissão de acesso nas chaves do Registro, nenhum usuário poderá salvar dados ali (nem mesmo o Administrador) e a mudança da permissão deverá ser desfeita caso haja necessidade de incluir algum novo arquivo.

As principais chaves utilizadas pelos malwares são:

Passo-a-passo
Para alterar a permissão no Windows XP ou Windows 2003, clique no botão Iniciar > Executar > digite **regedit** e tecle <enter>. No Windows NT e Windows 2000, você deve substituir regedit por **regdt32** e a opção de permissões está no menu Segurança.

Ao abrir o programa, você notará à esquerda cinco chaves:

HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

Ao dar um duplo-clique em qualquer uma das chaves, abrirá uma árvore com mais chaves e com isso você pode "navegar" dentro da árvore, indo para a chave desejada.

Nesta fase nós utilizaremos apenas duas chaves: **HKEY_CURRENT_USER**, abreviada para **HKCU**, e **HKEY_LOCAL_MACHINE**, abreviada para **HKLM.**

Uma das chaves que será modificada é a **HKCU\Software\Microsoft\Internet Explorer\Main** e portanto vamos usá-la como exemplo.

Você deve dar um duplo-clique em HKEY_CURRENT_USER, depois disso procurar ali dentro a chave Software e dar um duplo-clique nela. Prossiga desta mesma maneira para Internet Explorer (que está dentro da chave Microsoft) e, por fim, Main, que está dentro da chave Internet Explorer.

Quando você clicar em Main, aparecerá na janela à direita uma série de variáveis com ícones vermelho e azuis - e isso é perfeitamente normal.

No caso desta chave (HKCU\Software\Microsoft\Internet Explorer\Main), as variáveis à direita definem a página inicial, página de busca e outras configurações do IE.

Alterando a permissão
Para alterar a permissão da chave HKCU\Software\Microsoft\Internet Explorer\Main, que é algo que desejamos fazer

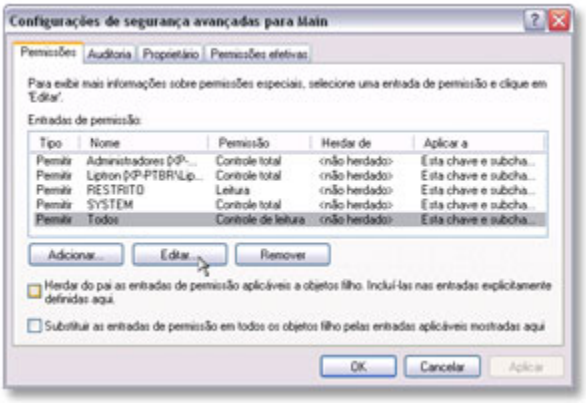
para evitar que as variáveis à direita sejam modificadas por qualquer malwares, você deve clicar com o botão da direita do mouse sobre a palavra Main (na árvore à esquerda) e escolher a opção *Permissões.*

Ao abrir a janela de Permissões, você verá os nomes dos grupos ou usuários. Como queremos impedir que *qualquer* usuário altere os dados da chave, vamos criar o grupo **Todos**, que conterá todos os usuários, e definir que este grupo não poderá modificar as variáveis, podendo apenas acessá-las (lê-las): desta maneira ninguém poderá alterar as variáveis, sendo que a única maneira de fazer isso será alterar a permissão desse grupo Todos.

Criando o grupo Todos
Clique no botão Adicionar e no campo que aparecer (abaixo da frase "*Digite os nomes de objeto a serem selecionados*"), digite a palavra "Todos" (sem as aspas).

Clique no botão Verificar nomes para confirmar que o grupo Todos está correto (note que agora a palavra Todos está sublinhada, indicando que o grupo foi reconhecido) e clique em OK.

Clique agora no botão *Avançado*. Clique na linha que contém a palavra Todos sob o campo Nome e clique no botão *Editar.*



Na lista que aparecer, clique no primeiro quadrado superior direito (Controle total / Negar) e todos os demais quadrados da coluna Negar serão ativados.

Como queremos permitir que as chaves possam ser lidas, desclique o segundo quadrado (*Consultar valor*) da coluna Negar e também a opção "*Enumerar Subchaves*" (para permitir que as sub-chaves existentes também possam ser lidas). O resultado final será o que você vê na imagem à direita: todos os quadrados da coluna Negar devem estar ativados, exceto os dois primeiros. Clique em *OK*. Agora você deve clicar na opção "*Herdar do pai as entradas de permissão aplicáveis ...*" e clicar na opção *Copiar* quando a janela de confirmação aparecer.

Clique em *OK* e aparecerá uma mensagem informando sobre a configuração de entrada de permissões. Isso ocorre

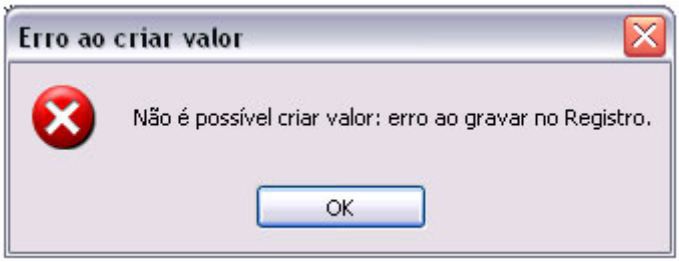
pois quando você cria uma permissão de negação, esta tem mais importância sobre entradas de permissão e com isso algumas funcionalidades poderão ser afetadas (e é justamente isso que queremos: proibir que as variáveis da chave possam ser alteradas). Clique em *Sim* para confirmar e, por fim, em *OK* para fechar a janela.

Ao seguir os passos acima, fizemos o seguinte:

1. Localizamos a chave HKCU\Software\Microsoft\Internet Explorer\Main
2. Criamos um usuário Todos
3. Fizemos com que o usuário Todos não tenha permissão para mudar a chave

Com isso, a chave HKCU\Software\Microsoft\Internet Explorer\Main está impedida de ser modificada. Para confirmar isso, tente criar uma nova chave dentro dela: na janela da direita, clique em qualquer espaço em branco com o botão da direita do mouse e escolha a opção *Novo* > *Valor da Seqüência*.

Aparecerá a mensagem abaixo, informando que não foi possível criar o valor - indicando que ninguém poderá modificar qualquer parâmetro na chave HKCU\Software\Microsoft\Internet Explorer\Main.



Desfazendo as alterações:
Caso você queira modificar algum parâmetro na chave HKCU\Software\Microsoft\Internet Explorer\Main, você deve simplesmente permitir a gravação de dados ali por Todos. Faça o seguinte:

1. Clique com o botão da direita do mouse em Main > Permissões ...
2. Clique em Todos e no botão Avançado
3. Clique na linha aonde Todos está no campo Nome e clique em Editar
4. Clique no primeiro quadrado abaixo de Permitir (Controle total) e todas as demais opções da coluna Permitir serão habilitadas.
5. Clique em OK, OK e novamente em OK.

Refazendo as alterações:
Após você fazer as modificações nas variáveis, é recomendável que você recoloque a permissão de negação na chave para garantir que nenhum programa possa mudá-la. Basta você seguir os passos abaixo:

1. Clique com o botão da direita do mouse em Main > Permissões ...
2. Clique em Todos e no botão Avançado
3. Clique na linha aonde Todos está no campo Nome e clique em Editar
4. Clique no primeiro quadrado abaixo de Negar (Controle total) e todas as demais opções da coluna Negar serão habilitadas.
5. Clique no segundo quadrado abaixo de Negar (Consultar valor) e na opção "Enumerar subchaves": com isso todas as opções da coluna Negar estarão habilitadas, exceto as duas primeiras e a "Enumerar subchaves".
5. Clique em OK, OK, Sim (confirmando a mensagem sobre permissão de negação) e novamente em OK.

Quais são as chaves que devem ser modificadas ?
Dependendo do grau de segurança desejado, aplique a modificação das permissões nas chaves abaixo, lembrando que **HKCU** indica a chave **HKEY_CURRENT_USER** e **HKLM** indica a chave **HKEY_LOCAL_MACHINE**:

Proteção mínima:
Suficiente para impedir que a maioria dos spywares e trojans se instalem:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

Proteção média:
Suficiente para impedir que a maioria dos spywares, trojans e hijackers se instalem:
HKCU\Software\Microsoft\Internet Explorer\Main
HKCU\Software\Microsoft\Internet Explorer\Search
HKLM\Software\Microsoft\Internet Explorer\Main
HKLM\Software\Microsoft\Internet Explorer\Search

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

Proteção máxima:
Impede que a maioria dos spywares, trojans e hijackers se instalem, bem como malwares mais sofisticados e difíceis de serem removidos. O ideal é que você também siga os próximos passos para manter a segurança máxima:
HKCU\Software\Microsoft\Internet Explorer\Main
HKCU\Software\Microsoft\Internet Explorer\Search
HKLM\Software\Microsoft\Internet Explorer\Main
HKLM\Software\Microsoft\Internet Explorer\Search

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices\
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Você deve aplicar nas chaves acima o mesmo passo-a-passo que foi aplicado na chave **HKCU\Software\Microsoft\Internet Explorer\Main** exemplificado acima.

15

Impedir que programas modifiquem arquivos no Menu Iniciar
Outra dica muito importante ajuda a evitar que malwares se instalem na pasta Iniciar do Windows, que é a pasta que aparece quando você clica no botão *Iniciar* > *Programas* > *Inicializar* e que mostra quais programas devem ser executados assim que o Windows for carregado.

Para impedir isso, seguimos o mesmo raciocínio da dica anterior: alteramos a permissão da pasta para evitar que qualquer programa seja adicionado ali.

> Os requisitos para esta dica são os mesmos da dica anterior: ela exige o uso do Windows NT, Windows 2000, Windows XP Professional ou Windows 2003 com partição NTFS no drive aonde o Windows está instalado, não estando disponível para Windows 9x/Me, Windows XP Home Edition, nem para qualquer versão do Windows instalado sob partição FAT32. Para você saber qual é a partição do seu drive, vá em *Meu Computador* > Clique com o botão da direita do mouse sobre a partição aonde o Windows está instalado (usualmente C:) > *Propriedades* e veja em *Sistema de arquivos* qual é o tipo de partição (FAT ou NTFS)

Alterando a Permissão da pasta Iniciar:
Existem duas pastas que mantêm a lista de arquivos que são executados na inicialização do Windows: a All Users, que contém a relação de programas que são executados para todos os usuários, e a pasta com o nome do Usuário que contém programas adicionais de acordo com cada usuário. As pastas são estas:

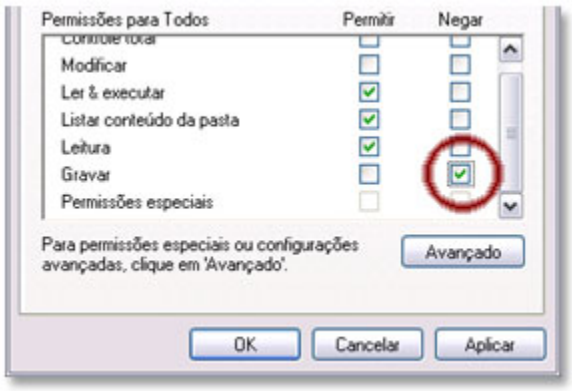
Windows em português:
- Todos os usuários: \Documents and Settings \All Users \Menu Iniciar \Programas \Inicializar
- Usuário específico: \Documents and Settings \(usuário) \Menu Iniciar \Programas \Inicializar

Windows em inglês:
- Todos os usuários: \Documents and Settings \All Users \Start Menu \Programs \Startup
- Usuário específico: \Documents and Settings \(usuário) \Start Menu \Programs \Startup

No Windows NT as pastas ficam dentro de WINNT/Profiles.

É importante que você modifique a Permissão de ambas as pastas, para uma maior segurança. Abaixo, utilizaremos como exemplo o Windows XP em português e a pasta \Documents and Settings \All Users \Menu Iniciar \Programas \Inicializar.

Navegue até a pasta \Documents and Settings \All Users \Menu Iniciar \Programas \Inicializar, clique com o botão da direita do mouse em qualquer espaço em branco da pasta e clique na opção *Propriedades*. Clique na aba *Segurança* e siga basicamente os mesmos passos da dica anterior: clique no botão *Adicionar* e no campo que aparecer (abaixo da frase "*Digite os nomes de objeto a serem selecionados*"), digite a palavra "Todos" (sem as aspas). Clique no botão Verificar nomes para confirmar que o grupo Todos está correto (note que agora a palavra Todos está sublinhada, indicando que o grupo foi reconhecido) e clique em OK. Tendo certeza que o usuário Todos está selecionado, clique na janela de Permissões o quadrado Gravar/Negar (veja imagem abaixo) para impedir a gravação de dados na pasta.



Mantenha as demais opções como estão.

Clique em *OK* e *Sim* (para confirmar a mensagem sobre permissão de negação) e agora a pasta não mais permite que seja salvo nenhum arquivo ali.

Desfazendo as alterações:
Caso você queira modificar algum programa na inicialização do Windows, basta você permitir a gravação de dados ali. Faça o seguinte:

1. Vá até a pasta correta: \Documents and Settings \(usuário) \Start Menu \Programs \Startup (para Windows em inglês) ou \Documents and Settings \(usuário) \Menu Iniciar \Programas \Inicializar (para Windows em português).
2. Clique com o botão da direita do mouse em uma área em branco > Propriedades
3. Clique na aba Segurança
4. Clique no usuário Todos
5. Desclique a opção Gravar na coluna Negar.
6. Clique em OK.

Refazendo as alterações:
Após você modificar algum programa na inicialização do Windows, é recomendável que você recoloque a permissão de negação na pasta para garantir que nenhum programa possa mudá-la. Basta você seguir os passos abaixo:

1. Vá até a pasta correta: \Documents and Settings \(usuário) \Start Menu \Programs \Startup (para Windows em inglês) ou \Documents and Settings \(usuário) \Menu Iniciar \Programas \Inicializar (para Windows em português).
2. Clique com o botão da direita do mouse em uma área em branco > Propriedades
3. Clique na aba Segurança
4. Clique no usuário Todos
5. Clique a opção Gravar na coluna Negar.
6. Clique em OK e Sim (para confirmar a mensagem sobre permissão de negação)

16

Impedir que programas modifiquem o arquivo HOSTS
Ao impedir que o arquivo HOSTS (dica 1) seja modificado, você terá mais segurança ao atualizar o Windows ou qualquer aplicativo via web pois você terá certeza que isso não será barrado por algum worm.

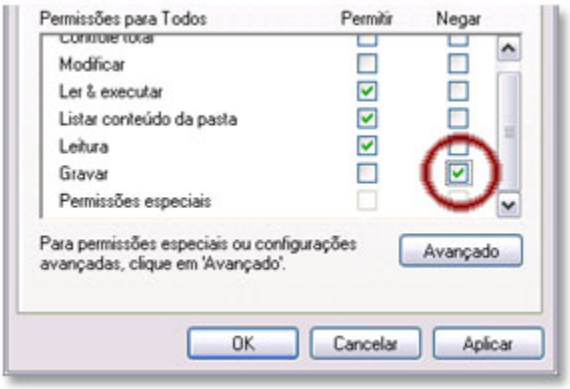
No Windows XP, o arquivo HOSTS (que não tem extensão) encontra-se em *\Windows\System32\Drivers\ETC* e no Windows 9x/Me ele está em *\Windows.*

Os requisitos para esta dica são os mesmos da dica anterior: ela exige o uso do Windows NT, Windows 2000, Windows XP ou Windows 2003 com partição NTFS no drive aonde o Windows está instalado, não estando disponível para Windows 9x/Me nem para qualquer versão do Windows instalado sob partição FAT32. Para você saber qual é a partição do seu drive, vá em *Meu Computador* > Clique com o botão da direita do mouse sobre a partição aonde o Windows está instalado (usualmente C:) > *Propriedades* e veja em *Sistema de arquivos* qual é o tipo de partição (FAT ou NTFS)

Navegue até a pasta aonde se encontra o arquivo HOSTS, clique com o botão da direita do mouse nele e escolha a opção *Propriedades*. Clique na aba Segurança e siga basicamente os mesmos passos da dica anterior: clique no botão *Adicionar* e no campo que aparecer (abaixo da frase "*Digite os nomes de objeto a serem selecionados*"), digite a palavra "Todos" (sem as aspas).

Clique no botão Verificar nomes para confirmar que o grupo Todos está correto (note que agora a palavra Todos está sublinhada, indicando que o grupo foi reconhecido) e clique em OK.

Tendo certeza que o usuário Todos está selecionado, clique na janela de Permissões o quadrado Gravar/Negar (veja imagem abaixo) para impedir a gravação de dados na pasta.



Mantenha as demais opções como estão.

Clique em *OK* e *Sim* (para confirmar a mensagem sobre permissão de negação) e agora o arquivo HOSTS não mais permite nenhuma alteração.

Desfazendo as alterações:
Caso você queira alterar o arquivo HOSTS (algo raro pois normalmente não há motivo para isso), basta você permitir a gravação de dados ali. Faça o seguinte:

1. Vá até a pasta aonde o arquivo HOSTS se encontra
2. Clique com o botão da direita do mouse em uma área em branco > Propriedades
3. Clique na aba Segurança
4. Clique no usuário Todos
5. Desclique a opção Gravar na coluna Negar.
6. Clique em OK.

Refazendo as alterações:
Após você alterar o arquivo HOSTS, é recomendável que você recoloque a permissão de negação na pasta nele para garantir que nenhum programa possa alterá-lo. Basta você seguir os passos abaixo:

1. Vá até a pasta aonde o arquivo HOSTS se encontra
2. Clique com o botão da direita do mouse em uma área em branco > Propriedades
3. Clique na aba Segurança
4. Clique no usuário Todos
5. Clique a opção Gravar na coluna Negar.
6. Clique em OK e Sim (para confirmar a mensagem sobre permissão de negação)

17

Como reconhecer um e-mail falso
Uma das principais maneiras de propagação de malwares é através de mensagens de e-mail com arquivos infectados - e estas mensagens estão cada dia mais criativas para fazer com que o internauta desavisado execute o arquivo anexo e seja infectado. As principais características desse tipo de e-mail são:

1. Mensagens com "cartões virtuais" ou com arquivos .scr, .pif, .ppt, .exe ou .zip

2. Mensagens "urgentes" do SERASA, de algum banco ou de alguma corporação

3. Mensagens da Microsoft informando sobre um importante update (pois a Microsoft JAMAIS envia arquivos anexados a mensagens) ou de empresas de antivirus (Symantec, McAfee e outras)

4. Mensagens com assunto "Urgente" que tenham arquivos anexados

5. Mensagens prometendo algum tipo de recompensa em dinheiro ou premiação

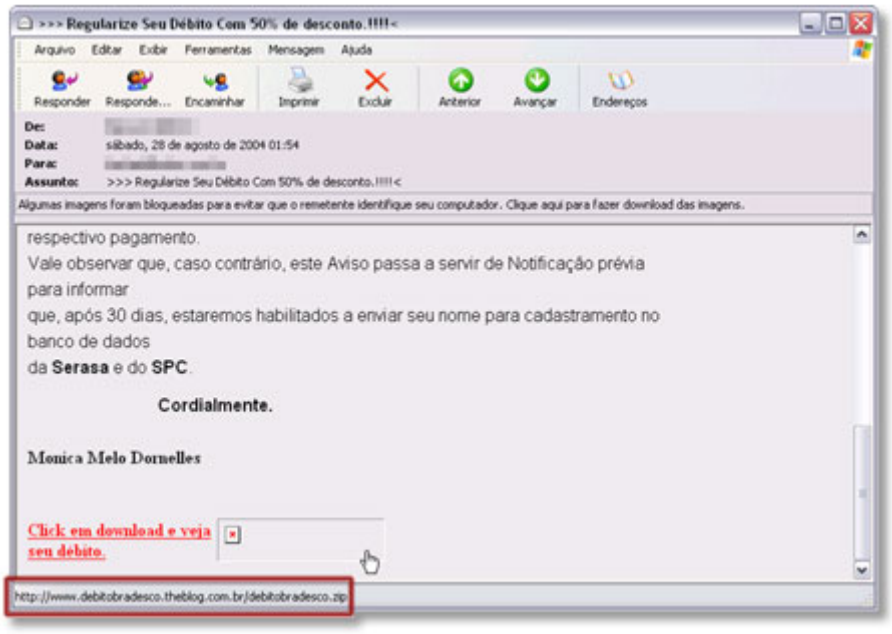
Há uma maneira bastante simples para identificar se o e-mail é falso: verificar qual é o link real para download do arquivo sugerido. Veja o exemplo abaixo: você tem uma mensagem de e-mail informando que o usuário recebeu um "cartão virtual" do site OCarteiro.com - mas ao manter o mouse sobre o link (SEM CLICÁ-LO), o endereço real aparece na barra.

Note que o endereço mostrado na barra não tem nada a ver com ocarteiro.com: o endereço ali é www.meumundo.americaonline.com.br /kalangoazsado/Cartao.exe, indicando que o site aonde o arquivo está hospedado não é ocarteiro.com, mas sim americaonline.com.br - algo que não tem nada a ver com o site original, comprovando que o e-mail é falso.

Mesmo que você se arrisque e faça o download do arquivo, um bom antivirus comprovará a farsa do e-mail, indicando que ele na verdade é um arquivo infectado com um malware (um trojan, neste caso):

Evidentemente se o seu antivirus está atualizado (passo 4), ele interceptará arquivos com malwares e evitará que você seja infectado - por isso um antivirus deve estar sempre atualizado ou ele não servirá para muita coisa.

Veja mais um exemplo abaixo, aonde o arquivo para "ver a dívida do SERASA" é obtido em um site que não tem absolutamente nada a ver com o SERASA: o site www.theblog.com (mais especificamente em www.debitobradesco.theblog.com.br/debitobradesco.zip), denunciando a falsidade da mensagem:



Para você saber qual é o site original aonde se encontra o arquivo para download, basta unir "www". com o site original (.com, .com.br ou qualquer que seja a extensão). Exemplos:

- **www.meumundo.americaonline.com.br**/kalangoazsado/Cartao.exe indica que o arquivo está hospedado no site **www.americaonline.com.br**.

- **www.debitobradesco.theblog.com.br**/debitobradesco.zip indica que o arquivo está hospedado no site **www.theblog.com.br**.

Tenha em mente que bancos e empresas grandes JAMAIS enviam arquivos via Internet e os links que constam nos seus e-mails são sempre do site da própria empresa. Além disso o site real é sempre aquele que tem a primeira extensão. Exemplos fictícios:

- **www.xyz.hehehe.com.br**/bradesco/mentira.htm é uma página do site **www.hehehe.com.br**

- **www.premios.badernov.com.br**/baboo.exe é uma página do site **www.badernov.com.br**

- **www.bradesco.cjb.com**/suaconta é uma página do site **www.bradesco.cjb.com** (que obviamente não tem relação alguma com o site do Bradesco: www.bradesco.com.br)

- **www.voceganhou.iitau.ru**/itau é uma página do site **www.iitau.ru** (que obviamente não tem relação alguma com o site do Itaú: www.itau.com.br)

- **www.files.co.uk/serasa.com.br/processo** é uma página do site **www.files.co.uk**

Veja alguns exemplos recentes de e-mails falsos:

- **E-mail falso (scam) usando o nome do Banco do Brasil**, aonde o link do "arquivo para atualização" é **http://www.minbo.com**/bbs/bb.com.br/gerenciadorfinanceiro/index.html, tentando enganar o internauta que lê "bb.com.br" no meio do link

- **E-mail falso (scam) usando o nome do site Humortadela**, aonde uma "página recomendada" é na verdade o arquivo **http://updatebr.net/**e/GBNTJ.exe

Seguindo essas dicas simples, a chance de você ser enganado é muito remota.

18

Configurações recomendadas do Windows
Um Windows bem configurado ajuda muito o usuário a evitar problemas de segurança e também de performance. Para isso, sugiro aplicar as seguintes dicas:

1. Ative as Atualizações Automáticas: vá no *Painel de Controle* > *Atualizações automáticas* > clique na opção *Automática (recomendado)* e defina qual é o melhor horário para a instalação de updates quando isso for necessário ou clique a segunda opção ("*Fazer download de atualizações para mim, mas permitir que eu escolha quando instalá-las*")
2. Se você quiser mais controle sobre o seu computador enquanto estiver navegando na web, o IE oferece adicionar a opção de Zona Meu Computador na aba Segurança, em adição às Zonas já existentes ali (Internet, Intranet Local, Sites confiáveis e Sites restritos).

Para habilitá-la, faça o download **deste arquivo .zip**, que contém um arquivo .reg que modifica um parâmetro no Registro do Windows, habilitando a Zona Meu Computador no Internet Explorer. Para isso, você deve dar um duplo-clique no arquivo zona_meu_comp.reg e aceitar a sua inclusão no Registro do Windows.

Embora as configurações dali não precisam ser modificadas, é importante saber que você tem acesso a configurações adicionais para aumentar a segurança

2. Restringir o tamanho máximo no Temporary Internet Files para 10 Mb, pois desta maneira os arquivos cacheados de páginas mais antigas serão eliminados, além de minimizar a fragmentação da partição. Para isso, faça o

seguinte: acesse o Internet Explorer > opção Ferramentas > na aba *Geral*, clique no botão *Configurações* que está dentro da área *Arquivos de Internet temporários:* altere ali o tamanho do espaço em disco a ser utilizado para 10 Mb.

3. No Outlook Express, impeça a visualização de imagens nas mensagens de e-mail para dificultar a sua identificação por spammers: vá no Outlook Express > menu *Ferramentas* > *Opções* > *Segurança* > clique a opção "Bloquear imagens e outros conteúdos externos em e-mails em HTML"

4. Ainda no Outlook Express, confirme se a opção "Zona de sites restritos" está selecionada na aba *Segurança.*

19

Tarefas semanais para manter o seu micro seguro
Agora que o seu computador está praticamente à prova de malwares, é muito importante que você mantenha-o assim para sempre. Para isso, é recomendável que você realize semanalmente as seguintes tarefas:

1. Acessar o **Windows Update** para verificar se há alguma atualização pois embora isso possa ser feito automaticamente via Atualizações Automáticas, é possível que haja alguma atualização não-crítica ou driver disponível para download

2. Rodar o Spybot ou o Ad-Aware (sempre verifique se há atualizações para eles antes de realizar a varredura de arquivos) para garantir que o seu sistema está limpo.

3. Limpar a pasta Temporary Internet Files acessando o IE > menu *Ferramentas* > na aba *Geral*, clique no botão *Excluir arquivos ...* que está dentro da área *Arquivos de Internet temporários*. Clique na opção para *Excluir todo o conteúdo off-line* e clique em *OK*.

20

Aonde se atualizar sobre malwares e vulnerabilidades ?
Existem diversos sites na web (todos em inglês) que mantém você informado sobre novas vulnerabilidades e malwares, sendo uma boa leitura caso você se interesse pelo assunto. Alguns deles:

Sites contendo as mais recentes vulnerabilidades:
- **Secunia**
- **SecurityFocus**
- **CERT**

Sites com os mais recentes malwares:
- **Symantec**
- **Sophos**
- **Topix**

Sites com notícias recentes sobre segurança:
- **eWeek**
- **CNET**
- **PC Magazine**

Dúvidas sobre malwares ?
- **Fórum do BABOO**, nosso Fórum gratuito aonde você obtém ajuda aos seus problemas e resposta às suas dúvidas sobre malwares.

Conclusão:
Como você pode observar nas dicas deste guia, não é difícil manter o Windows praticamente imune a malwares: é apenas um pouco trabalhoso para quem nunca se preocupou com isso.

Excetuando a dica 14 (detalhando a mudança de permissão de algumas chaves do Registro do Windows, que é a solução mais complexa e eficiente para impedir a instalação de malwares no computador), as demais dicas são bastante fáceis e simples de serem implementadas.

Há tempos a Microsoft iniciou uma campanha ressaltando 3 etapas para manter o seu computador seguro:

1. Usar um firewall
2. Manter o Windows atualizado
3. Manter o antivirus atualizado

Embora estas três dicas sejam suficientes para manter o seu computador seguro, os malwares estão ficando cada vez mais sofisticados e criativos, exigindo um cuidado maior para evitar que eles infectem o seu computador.

A midia especializada adora mostrar casos escabrosos de prejuízos bilionários que empresas têm com vírus, worms e malwares em geral, mas ignora que há milhões de computadores que não sofrem problema algum com isso. E é por este motivo que eu criei este Guia: fazer com que você faça parte do grupo que não se preocupa mais com malwares, tendo conhecimento deles apenas ao ler notícias sobre algum malware novo que apareceu na web !

Eu espero que este Guia ajude o internauta brasileiro a se proteger contra qualquer tipo de malwares, aumentando (e muito !) a segurança do seu computador contra estas pragas. Por isso, este Guia pode (e deve) ser distribuído livremente para que todos possam aproveitar ao máximo as dicas aqui postadas, fazendo com que o Brasil não seja um dos campeões de computadores infectados, como ocorre hoje.

O Guia Definitivo para Detecção, Eliminação e Proteção contra Malwares será atualizado sempre que for necessário (quando houverem novas versões dos programas citados) e para obter a versão mais recente deste guia, acesse a página http://www.baboo.com.br/malware.

Este guia te ajudou ? Queremos saber ! Envie suas críticas ou elogios para malware@baboo.com.br. Dúvidas sobre o conteúdo deste guia devem ser postadas no Fórum do BABOO pois não respondemos dúvidas via e-mail.

Obrigado pelo seu tempo e até a próxima !

Baboo.
www.baboo.com.br
BABOO/MSN
MVP Windows

Guia Definitivo para Detecção, Eliminação e Proteção contra Malwares
Abaixo você tem a lista das atualizações deste guia, sendo que o número entre parênteses indica o número da dica (1 a 20):

Versão 1.2: 31/08/04
- adição da informação sobre as dicas 15 e 16, que não funcionam com o Windows XP Home Edition
- correção da informação sobre o Adware Away, que é um programa trial e não gratuito (11)

Versão 1.1: 30/08/04
- adição de quatro linhas de Registro (12)
- adição de uma dica sobre Outlook Express (19)
- adição de dica com imagem sobre a Zona Meu Computador (19)
- informações adicionais sobre o Spybot (8)
- adição de informação sobre o uso do regedt32 no Windows 2000 (12)
- inclusão de mais exemplos de e-mails falsos (17)
- inclusão dos arquivos para download (Introdução)

Versão 1.0: 28/08/04
Primeira versão do Guia.

Algumas dicas e correções foram sugeridas pelos participantes E-ponto, glenio, pccariocadc, itapira e Mr.Million do Fórum do BABOO.