Perdendo a inocência

Saiba quais são os reais riscos que assombram as redes de computador

por Ricardo C. Zimmerl

No artigo anterior, abordei uma forma de navegar na Internet com mais segurança sem, contudo, perder as funções necessárias para aqueles sites que precisamos acessar e sobre os quais temos alguma confiança. Mas quais são os riscos que corremos quando temos nosso computador conectado a uma rede? Quais são os verdadeiros e ocultos perigos que nos rondam quando acessamos um site ou baixamos um e-mail? A desinformação nessa área é muito grande e, portanto, cabe um esclarecimento destes riscos.

A indústria de informática sempre alerta para o perigo dos downloads e cópias de softwares piratas devido ao risco de trazerem vírus, o que realmente ocorre, mas, muitos softwares gratuitos tornam-se um verdadeiro pesadelo para quem quer economizar algum dinheiro. Como diz o ditado: "o barato sai caro" e vários softwares e plug-ins de algumas empresas de renome também podem prejudicá-lo – e muito!

Conhecendo o inimigo

Primeiramente, vamos analisar os riscos e aprender o que realmente eles são:

Vírus

Os vírus são programas de computador capazes de se infiltrar em outros programas efetuando cópias de si mesmos, podendo ou não ter outras ações maléficas.

Vírus especiais

Vírus de macro, script ou class. São vírus que não infectam programas comuns e sim arquivos específicos que podem ser executados, como os arquivos CLASS do Java ou documentos do Word. Vírus de script podem infectar páginas de Internet e e-mails.

Worms

Muitas vezes chamados de vírus, mas diferem desses por não serem capazes de se infiltrar em outros programas. Os worms são programas autônomos que operam de forma isolada. Para garantir que serão executados, todos os worms precisam se instalar em entradas de inicialização do sistema (o software *Alerta-Z*, permite monitorar as principais entradas e, conseqüentemente, detectar e neutralizar a maior parte dos worms que existe ou que venham a existir). Um worm pode conter comandos destrutivos, backdoors (deixam uma porta do computador aberta para permitir invasões), trojans ou apenas se replicar.

Trojans

Também conhecidos como Cavalos de Tróia. São programas que, uma vez instalados no micro, permitem a invasão de hackers, dando a eles o poder de controlar algumas (ou várias) coisas em seu computador.

Spywares

Os famosos softwares de espionagem. São softwares que espionam o que você faz durante a navegação, mas, que, também, podem espionar o que você tem no computador, roubar suas senhas, números de cartões de crédito e muito mais.

Mesmo alguns plugins ou softwares costumam monitorar o uso que se faz deles (quais sites você navega, dados de seu computador, quantas vezes ativa o produto ou quais recursos usa com mais freqüência para "efeitos de marketing" ou de melhoria dele enviando essas informações à empresa produtora, o que não deixa de ser espionagem e perda de privacidade).

Keyloggers

Spywares muito específicos, destinam-se a gravar tudo o que você digita em seu micro, indicando, em alguns casos, qual o software ativo quando você digitou, endereço de site, se foi um navegador e até monitorando a área de transferência, caso você copie um texto para ela. Depois enviam essas informações para um endereço determinado ou, simplesmente, as deixam armazenadas para posterior "consulta" pelo bisbilhoteiro.

Adware

Costuma tornar as vidas de muitos um inferno, abrindo incontáveis janelas do navegador em endereços de sites muitas vezes pornográficos. São softwares criados para gerar "tráfego", mesmo que falso, já que as pessoas não vão ficar olhando aquelas páginas, fazendo com que seus autores ganhem "um troquinho" com isso.

BadCOM

São arquivos BAT compilados. Podem conter comandos destrutivos ou simplesmente aborrecer os usuários com menos conhecimento em informática. Um truquezinho que inferniza a muitos é a criação de um BadCOM com nome **Win.com** e a troca do original (que é o inicializador do Windows) pelo BadCOM, que normalmente exibe uma mensagem. Sem o **Win.com** verdadeiro, o Windows não inicia. Não adianta usar um antivírus, pois, BadCOMs não são detectáveis por eles. Aí, o que as pessoas fazem é formatar o HD e reinstalar o Windows quando a única coisa necessária a ser feita é arrumar um arquivo win.com com alguém que tenha a mesma versão do sistema operacional ou extraí-lo do seu CD original do Windows. É um arquivo pequeno e cabe em um disquete. Basta sobrepô-lo ao falso, na pasta **C:\Windows** (o C é a letra da unidade onde está seu sistema).

Arquivos especiais

Existem muitos tipos de arquivos que podem ser executados, como PIF, LNK, WSC, SCT, etc., e, com isso, conter ou acionar códigos perigosos. Inclusive os arquivos PDF ou SWF tiveram essas falhas já exploradas por worms e por vírus. Tenha sempre em mente uma coisa: o perigo existe e sempre existirá onde for possível executar comandos, principalmente de *shell* (abrir/acionar arquivo).

Sniffers (farejadores)

São programas que permitem pegar pacotes de informação em tráfego numa rede e analisá-los. Essa descrição básica é essencial para entendermos o resto de nossa explicação.

Podemos concluir que temos perigos que rondam a comunicação (sniffers), perigos que podem estar nas páginas que acessamos, em nossos e-mails e em nosso computador, mas, como determinar exatamente onde eles estão?

Embora existam sniffers para a Internet (WAN), o maior perigo é o uso de sniffers em redes internas (LAN), já que pela Internet é um jogo de acaso, devido ao enorme tráfego e à normal variação do IP, quando a conexão é discada, mas mesmo para IPs fixos (conexão DSL) o uso de sniffers só é algo fácil se empregados no servidor, sendo muito complicado para um computador remoto.

Existem softwares que permitem a detecção de programas sniffers em redes internas, mas, em rede WAN (Internet), o melhor meio de se proteger é sempre passar senhas e números de cartões somente em sites que oferecem comunicação segura (como padrão SSL), isso pode ser verificado quando um cadeado aparece na barra de status do Internet Explorer, por exemplo.

Se a conexão não for segura, as informações poderão estar sendo "farejadas" por um "bisbilhoteiro" em algum lugar do mundo. Muitos de vocês talvez se preocupem com a falta de privacidade que os cookies causam, não?

Vamos aos fatos. Antigamente (antes do ASP), muitos sites usavam os cookies como forma de armazenar informações de compra, o que, sem dúvida, era incômodo e potencialmente perigoso. Hoje, o maior problema dos cookies não está exatamente relacionado a mostrar quantas foram as vezes que você visitou tal site ou quais páginas você acessou, mas, sim, armazenar em seu computador senhas de acesso, como, por exemplo, a sua senha de e-mail. Muita gente, por comodidade (entenda-se preguiça), não gosta de digitar a senha toda hora que acessa o e-mail ou entra em sites com acesso restrito e opta por salvar a senha ou "lembrar senha neste computador". Para que o site ofereça esse serviço, ele tem que gravar um cookie com esses dados. É aí que mora o perigo, pois, outra pessoa, ao acessar o site, não precisará saber a senha e terá o acesso garantido por causa dos cookies.

É claro que os cookies ocupam espaço no HD, não muito, é verdade, mas ficam ocupando; e quanto mais limpo estiver o HD de nosso computador, tanto mais rápido e eficiente ele será. E como os cookies são dispensáveis, é sempre interessante executar uma faxina periódica.

Todos fazem um enorme terrorismo relativo aos e-mails com vírus ou anexos perigosos, mas, há um outro perigo enorme, para quem costuma navegar muito, até maior que o dos e-mails e que, geralmente, é ignorado: os controles Active-X e Java.

Um controle Active-X é um programa de computador, como qualquer outro. Quando você acessa uma página que usa um controle desses, o programa é executado, e adivinha onde? Em seu micro!

Pois é. Se esse controle possuir um vírus, contiver um trojan ou ele próprio for maldoso e capaz de roubar suas senhas, o que você acha que irá acontecer?

Exatamente. Você pode ter seu computador infectado por um vírus apenas por ter acessado uma página de Internet que usa um controle Active-X contaminado. Na minha coluna anterior, eu mostrei como neutralizar essa ameaça, portanto, não serei redundante. Mas existe um outro problema: os controles Java.

Muitos sites oferecem joguinhos em Java ou têm algum recurso que usa o Java (são os famosos arquivos CLASS), o problema é que existem códigos maliciosos em Java e "vírus" também, e normalmente os antivírus não oferecem proteção contra esses scripts.

Isto também é uma questão de escolha: se você quer segurança remova a máquina virtual Java de seu computador ou, pelo menos, desabilite o Java de seu navegador.

Parecidos com esses vírus em Java existem os vírus de script (VBS), como os famosos "I Love You", "Melissa", entre outros. Esses vírus podem vir como anexos de e-mail, mas, também, podem ser acionados por páginas da Internet. Como os vírus em Java, é fácil estar bem protegido contra esses scripts, pelo menos em versões do Windows até o 98. Basta remover o "Windows Scripting Host". (**Menu Iniciar**, **Configurações**, **Painel de controle**, **Adicionar remover programas**, **Instalação do Windows**, **Acessórios**, **Detalhes**).

Remover o Windows Scripting Host não costuma acarretar qualquer problema ao usuário, pelo contrário, previne muita dor de cabeça, mas, se algum programa parar de funcionar corretamente é só reinstalá-lo. Quanto aos e-mails e seus anexos, essa é uma história já bem conhecida e o que se pode recomendar é: prefira um webmail a um e-mail baseado em seu computador (como o Outlook, IncrediMail, etc.), caso você precise de um software de e-mail em seu micro, dê preferência a outros softwares, como o Eudora, em vez do manjado Outlook. Mas lembre-se de que o perigo também mora ao lado. Algum "amigo", colega de trabalho, chefe, pode muito bem instalar um software trojan ou vírus em sua máquina quando você estiver ausente (para te ajudar com isso, o Alerta-Z tem uma função de bloqueio do micro, não tenha preguiça de usá-la), e lembre-se de que trojans e worms precisam iniciar com o sistema.

Utilize as funções do Alerta-Z aumentar a segurança da sua máquina. Monitore os aplicativos em seu micro (recurso **anti-freeze**), veja quem está conectado à sua máquina (recurso **Active Connections**), tome alguns cuidados para poder navegar tranqüilo.

Mantenha seu antivírus atualizado, sempre use um bom firewall quando estiver em rede e aprenda a usar o Alerta-Z. Creia-me ele pode ser um verdadeiro anjo da guarda digital pois nem sempre seu micro é infectado depois que criaram as vacinas, então não adianta ficar sempre para trás, é melhor contar com uma ferramenta que possa ajudá-lo a enfrentar essas ameaças digitais, quer sejam conhecidas ou não.