Manual Anti-hacker

Como proteger o seu sistema de ataques e invasões

André Valle, Claudia Guimarães e Fabricio Chalub

Capítulo 1

Introdução

Com o advento cada vez mais disseminado de conexões dedicadas à Internet, o número de invasões de computadores pessoais por hackers (ou mais precisamente, crackers) tem aumentado de maneira assustadora.

Antes restritos ao ambiente corporativo, os criminosos digitais agora voltam suas armas e técnicas para o usuário doméstico.

Como fazer para se proteger. Esta pergunta nos é feita diariamente, e desta forma, de comum acordo com a editoria da revista Internet.br, resolvemos escrever este pequeno guia que, se garantidamente não o protegerá de todos os perigos (nenhum sistema é 100% seguro), certamente diminuirá muito a sua probabilidade de ser atacado com sucesso.

Dividimos o texto em diversas seções, permitindo que sejam tomadas diversos tipos de precauções relacionados com as várias aplicações utilizadas hoje

em dia pela maioria dos usuários da Internet brasileira.

Desta forma, iniciamos o texto mostrando a anatomia de um ataque, passando pela proteção a ataques por correio eletrônico, e posteriormente permitindo o uso de técnicas para defesa em sistemas de chat (IRC) e de mensagens instantâneas (ICQ). Também são abordados sistemas de proteção contra Applets Java e Controles ActiveX, além de soluções de segurança através de firewalls pessoais.

E, ao contrário de algumas publicações atualmente no mercado editorial, este não é um documento escrito por hackers (talvez os mais atentos notem isso pela qualidade gramatical … :) para aprendizes de hackers, e sim um documento técnico cujo objetivo é auxiliar o usuário doméstico (e também o corporativo, por que não?) a se proteger de uma série de ataques realizados por estes autênticos criminosos desta nova era online.

Mas infelizmente, ao contrário de outros artigos e livros publicados anteriormente, neste caso não poderemos garantir 100% de satisfação ao usuário

final. Afinal, como qualquer especialista neste assunto sabe muito bem, não se pode provar que um sistema é seguro, e sim que é inseguro.

E com certeza, a busca de resultados cada vez melhores é um fator que vai depender quase que exclusivamente de um desejo pessoal de aprimoramento e busca por novas informações, já que desde a entrega deste texto aos editores até a sua publicação, dezenas de novas falhas de segurança em inúmeros sistemas operacionais e softwares terão sido descobertas.

Capítulo 2

Tipos de ataques

Uma pequena descrição da família de protocolos TCP/IP

Para entender como ataques funcionam, é necessário ter uma pequena noção de como trabalha a Internet, ou pelo menos, como a sua base de protocolos de comunicação. Esta família de protocolos é chamada de TCP/IP. Como sabemos, cada computador ligado à Internet é identificado por um número IP. A maioria das pessoas conectadas não têm um número IP fixo; ao contrário, toda vez que se conectam ao seu provedor recebem um novo número.

Apesar de um número IP ser utilizado para identificar uma máquina dentre as milhões conectadas à Internet, ele não é suficiente para que esta máquina troque informações com as outras. Por exemplo, um mesmo endereço IP, 192.168.1.1, pode ser usado tanto para conexões via browser (WWW), FTP e IRC. Como um cliente do serviço WWW pede uma página

para esta máquina? E como a máquina 192.168.1.1 diferencia seus diferentes servicos oferecidos à Internet? É aí que surge um importante conceito, muitas vezes negligenciado pelos usuários, mas que é vital para compreender os vários tipos de ataques de crackers, que é o de "porta". Agora, além de identificarmos as máquinas da Internet, podemos identificar os serviços prestados por elas, e cada um deles é identificado com um número diferente. Estes números são padronizados, para evitarmos confusão. Por exemplo, para utilizar o serviço WWW da nossa máquina 192.168.1.1, basta abrirmos uma conexão com a porta 80. O FTP utiliza a porta 21, o ICQ usa portas na faixa 1000–2000 e o IRC as portas 6666, 6667 e 6668. Existem um total de 65535 números disponíveis para serem utilizados em uma única máquina. Quando mais serviços a máquina oferece, mais portas (e seus números) são disponibilizados. Até mesmo a sua máquina Windows 95/98, que aparentemente não fornece serviço nenhum tem portas abertas.

A coleta de dados

Um ataque bem sucedido a um computador é aquele que explora uma vulnerabilidade existente em um programa (ou serviço) rodando na máquina. Como já dissemos antes, a maioria dos serviços são acessados através da camada TCP/IP, e são identificados por um número de porta. Ataques ao próprio mecanismo de manipulação do protocolo TCP/IP também são freqüentes, como iremos ver a seguir.

Para que um invasor possa explorar as falhas de seguranças nos vários sistemas de sua máquina, ele precisa saber antes o que está disponível. Existem dois métodos bastante utilizados para este tipo de coleta de dados: a varredura de portas (*port scan*) e a impressão digital (*fingerprint*) do sistema operacional.

Port scans

utilizando programas especiais, o invasor lança sondas (pacotes IP especiais) tentando estabelecer uma conexão com cada uma das 65535 portas do seu computador. Se existe algum serviço associado

a uma porta, ele irá responder. Desta maneira, o invasor consegue saber, em poucos segundos, o que você está rodando em sua máquina.

Impressão digital (*fingerprint*)

Através do envio de uma sequência especial de pacotes IP a um site específico, pode-se detectar que sistema opercional está rodando analizando os pacotes que ele envia de volta.

Com posse destas informações, ele já sabe que ferramentas utilizar para tentar invadir ou vandalizar o seu micro. E é neste ponto em que você deve prestar muita atenção. A informação é a alma do negócio. Invasão de sistemas é basicamente uma tarefa de pesquisa e coleta de dados. Quanto mais informado e atualizado você estiver, menos chances você terá de sofre algum tipo de ataque no futuro.

Ping sweep

O “ping” é um comando de protocolo que verifica se um computador está vivo ou não. Um cracker pode varrer centenas de possíveis endereços e saber em

pouco tempo quais máquinas estão conectadas à rede.

Verificação de contas

Sistemas operacionais voltados para rede, tipo Windows NT, Linux e variantes do BSD vêm com contas pré-definidas (ex.: Administrator, root, bin, games, etc).

Muitas vezes, a instalação destes sistemas operacionais não segue algumas regras básicas de segurança, como a não colocação de senhas para estas contas *default*. Também são comuns senhas ridiculamente fáceis de serem adivinhadas. Um cracker paciente pode tentar por várias horas até encontrar uma máquina com este tipo de problema, utilizando um pequeno programa que checa estas vulnerabilidades automaticamente.

Potes de mel

Um termo muito usado no meio de segurança é o chamado “pote de mel” (*honeypots*), também conhecido por “doce” (*candy bar*), que são programas que fingem ter uma certa vulnerabilidade de forma a

atrair um possível invasor. Desta maneira conseguimos identificar um invasor antes que ele explore uma vulnerabilidade do seu sistema. Por exempo, o **NoBO,** disponível no endereço http://web.cip.com.br/nobo/, é um programa que simula a presença de um conhecido cavalo-de-tróia (**BackOrifice**), e informa o usuário quem está tentando invadir a sua máquina.

Figura 02_01 – O NoBO em ação

Outro programa deste tipo, para o cavalo-de-tróia **Netbus** é o **Netbuster**, disponível em http://softwaresolutions.net/netbuster.htm.

Sniffers, farejadores de pacotes

Uma maneira muito simples de se obter senhas é através da técnica conhecida como *sniffing*. *Sniffers*

são programas que capturam todos os pacotes que passam pela rede, sejam eles destinados a sua máquina ou não (diz-se que a sua interface de rede está operando em modo *promíscuo* — aceitando todos os pacotes que ela enxergar). Não se preocupe: é muito difícil um cracker capturar pacotes de um provedor; esta técnica é mais comum em ambientes corporativos ou em laboratórios de computadores, onde existe uma rede local (LAN) Ethernet. Neste caso o perigo é real e imediato. Qualquer conexão onde você é obrigado a enviar a sua senha pela rede pode ser capturada. Alguns casos em que a senha é enviada em aberto:

- Servidores de FTP
- Autenticação de usuários NT (utilizando a opção menos segura)
- Servidores de TELNET
- Servidores de EMAIL

Outra maneira de lidar com farejadores é utilizando programas que detectam este tipo de atividade. Através de técnicas especiais, você pode detectar

quem da sua rede está operando em modo suspeito. Um excelente programa é o AntiSniffer, disponível para download no endereço http://www.lopht.com/antisniff/.

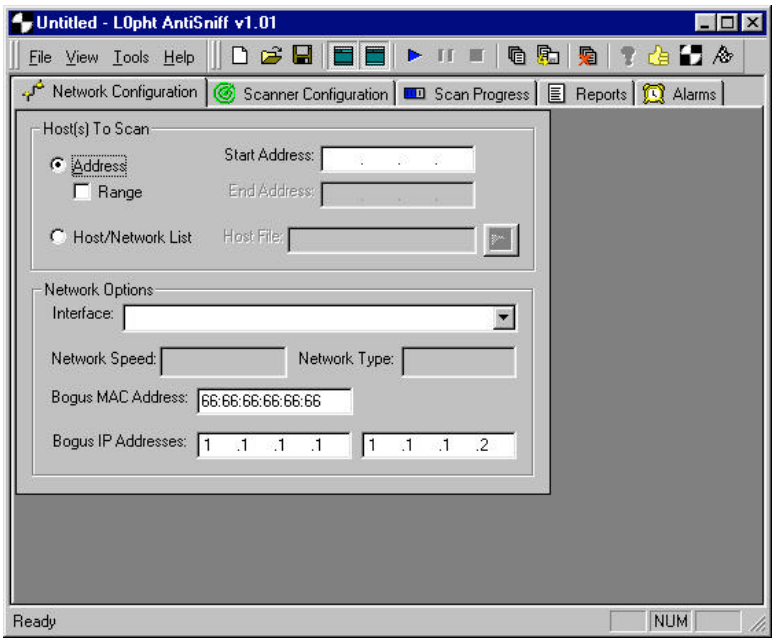

Figura 02_02 – O AntiSniffer

Crashes e telas azuis da morte

Esta é uma categoria conhecida, na área de segurança, como ataques DoS. Este termo vem de “Denial of Service”, ou negação de serviço. São formas e técnicas de fazer com que um determindo serviço (possivelmente a máquina inteira) fique

inoperante. Muitos dos ataques que iremos descrever abaixo têm soluções disponíveis, bastando para isso você utilizar as últimas atualizações de segurança do seu sistema operacional.

ICMP DoS: Um pacote construído maliciosamente pode causar um crash em máquinas Windows 95. Para corrigir este problema, baixe o arquivo ftp://ftp.microsoft.com/Softlib/MSLFILES/vipupd.exe e atualize o seu sistema. Máquinas Windows 98 não são afetadas.

SYN Flood: ou Inundação de SYNs. SYNs são pacotes IP especiais que abrem uma conexão. Enviando uma chuva desses pacotes em um curto espaço de tempo, o sistema abre muitas conexões com a máquina alvo e não fecha nenhuma. Consequentemente o sistema não consegue mais utilizar a rede.

Land, Latierra, WinNUKE, OOB, Teardrop: formas de construção de pacotes de forma a travar seu micro. Não afetam máquinas Windows 98. Para os usuários do Windows 95, o seguinte arquivo deve ser

instalado em sua máquina: ftp://ftp.microsoft.com/softlib/mslfiles/msdun13.exe.

Smurf: este tipo de ataque não tem remédio. Sua rede é inundada por pacotes deixando a sua conexão muito lenta e até mesmo inoperável. Este ataque é muito sério, mas é mais direcionado a sites. Raramente usuários de provedores sofrem com isso. Se você acha que está sob um ataque Smurf, ou seja, se você está notando que sua conexão com a Internet está cada vez mais lenta, apenas reconecte-se ao seu provedor.

Capítulo 3

Mantendo seu sistema seguro

Existem atualmente 41 tipos de vulnerabilidades conhecidas publicamente que afetam sistemas Windows 95 e 98. Muitas dessas já são velhas conhecidas e têm soluções que são publicadas pela Microsoft em seu site.

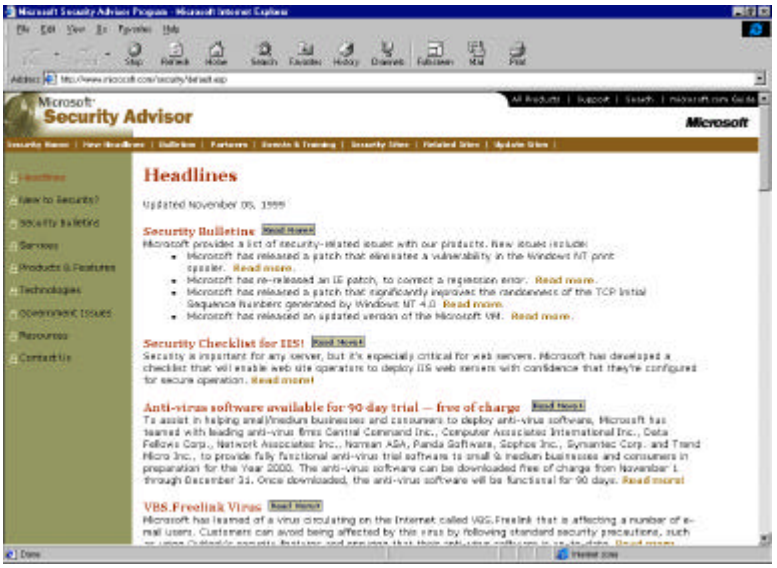

Figura 03_01 – O site Security Advisor, da Microsoft

Portanto, recomendamos que você fique atento aos avisos divulgados pela Microsoft no endereço http://www.microsoft.com/security. Usuários do Windows 95, versão inglês, devem ir para

http://www.microsoft.com/windows95/downloads e usuários do Windows 98, para http://www.microsoft.com/windows98/downloads. Nestas páginas, recomendamos que sejam feitas todas as atualizações recomendadas sob o tópico “Critical Updates”. Para downloads em português, vá para http://www.microsoft.com/brasil/download/?MSCOMTB=ICP_Downloads.

Outra fonte inesgotável de avisos e recomendações é o site Security Focus. Independente de qualquer fabricante, o site, localizado no endereço http://www.securityfocus.com, oferece uma lista quase que interminável de falhas de segurança em diversos sistemas operacionais.

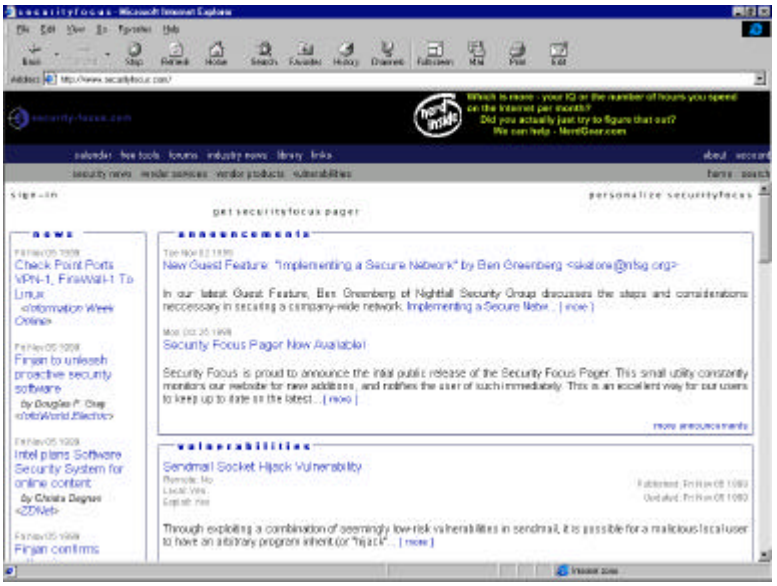

Figura 03_02 – O site independente Security Focus

Além disso, eis o que você pode fazer para manter o seu sistema seguro:

? Desabilite o compartilhamento de impressoras. Quando este compartilhamente é ativado, o sistema cria um compartilhamento (share) chamado PRINTER$, permitindo que sistemas remotos acessem drivers de impressoras do diretório de sistema local. Infelizmente este mesmo compartilhamento permite que outros tipos de arquivos sejam acessados de maneira maliciosa.

- Desabilite o compartilhamento de arquivos. Como usuário de um provedor, não há a necessidade de ter arquivos compartilhados, já que você é o único que usa o seu computador! SE você tem uma rede caseira, utilize senhas complicadas e apenas ligue o compartilhamento quando necessário!

- O Windows guarda as senhas mais recentementes utilizadas no sistema, por isso, apague regularmente os arquivos com extensão .PWL no diretório C:\WINDOWS.

- Nunca faça o download de programas fora do site original. Por exemplo, você descobriu uma versão nova do ICQ em um site pessoal de alguém, ou uma versão mais atual do mIRC que você não conhecia. É tentador baixar estes programas para ficar sempre atual, mas você nunca deve fazer isto, já que muitos vírus e cavalos-de-tróia são disseminados desta forma. Caso você desconfie que uma versão mais nova do seu programa favorito foi lançada, vá ao site original dele e verifique isso.

Se você descobriu uma versão mais nova de um programa e quer inserí-la no seu site para que seus usuários façam o download, coloque um link para o site original, com instruções de como obtê-lo.

Capítulo 4

Segurança no email

Como livrar-se de vírus e cavalos-de-tróia

Primeira e única regra para manuseio de emails:

Nunca abra arquivos anexados a mensagens

Arquivos anexados a emails podem carregar vírus e cavalos-de-tróia que, ao serem executados, infectarão o seu computador, com consequências imprevisíveis. Existe uma mania de se distribuir pequenos programas executáveis que, quando abertos, mostram uma pequena animação ou contam alguma história engraçada. Ignore estes emails, mesmo se foram enviados por conhecidos. Em relação a arquivos-documento, tenha a mesma precaução. Documentos Office (Word, Excel, Powerpoint, Access) podem conter vírus em forma de macros que infectam o seu computador assim que os arquivos são abertos nos respectivos programas. Estes virus ficam residentes nos arquivos de gabarito

normal.dot e se espalham sempre que você distribui um novo documento.

Passe um anti-vírus em todos os arquivos que receber por email e mantenha-o atualizado para que ele detecte todos os novos tipos de vírus que são produzidos quase diariamente.

Existem mais de 30 tipos de cavalos-de-tróias atualmente na Internet. O Netbus, BackOrifice, o Happy99, o Xmas, o Melissa são apenas **alguns**. Lembre-se disso!

O que é um vírus

Um vírus pode ser definido como um programa de computador que infecta outros programas, modificando-os para incluir uma cópia de si mesmo. Em outras palavras, todos os vírus se copiam, sendo que alguns, para despistar, modificam-se ligeiramente. Esta característica de mutação dificulta a ação de programas anti-vírus.

Estatisticas mostram que somente 5% dos vírus contém algum código que é considerado maligno, ou seja, interfere no funcionamento do seu computador,

como uma mensagem na tela ou o inteiro apagamento do seu disco rígido.

Na maioria das vezes, os vírus utilizam uma data alusiva a algum evento para disparar o seu efeito, como as famosas sextas-feitas 13.

Como tudo começou

Muitas pessoas nos perguntam como esta história começou. É um pouco difícil precisar a data exata, mas sabe-se que na década de 60, nos mainframes (grandes computadores) programadores criavam softwares de batalha, que ficavam guerreando uns com os outros. Já nos anos 80, foram achados os primeiros vírus modernos, rodando nos velhos Apple II.

Em 1983, o termo vírus de computador foi definido pelo pesquisador Fred Cohen, e se passaram 3 anos até o primeiro vírus para PC surgir. Era o Brain, inútil e inofensivo, mas se escondia facilmente e era bem difícil de se achar.

Em 1988, os softwares anti-vírus se tornaram uma febre, e até a Microsoft os incluiu na versão 5.0 do seu DOS.

Em 1992, surgiu o primeiro vírus famoso, o Michelangelo. Talvez devido ao nome, teve uma excelente cobertura na imprensa e as vendas de anti-vírus explodiram.

Em 1995, uma nova geração de vírus surgiu, baseada na linguagem de programação de macros do Microsoft Office. Ao contrário dos antecessores, estes exemplares eram disseminados através de documentos, principalmente do Microsoft Word.

Os vírus e a Internet

Com a popularização da Internet, as possibilidades de contaminação foram multiplicadas, já que o download, um processo que praticamente era restrito aos poucos frequentadores de BBS (uma espécie de quadro de avisos eletrônico, que agregava mensagens e programas), passou a ser utilizado diariamente por milhões de pessoas.

Estima-se que atualmente 80% das contaminações por vírus ocorra através da transmissão de arquivos pela Internet. Além disso, segundo o Centro Nacional para Crimes de Processamento de Dados, nos Estados Unidos, a economia americana perde anualmente cerca de US$550.000.000 em prejuízos causados por vírus, sem contar as horas perdidas nas tarefas de recuperação de dados e programas.

Os tipos de vírus

Os vírus podem ser catalogados em 3 categorias básicas:

Vírus de boot

Os vírus de boot são transmitidos basicamente por disquetes, copiando-se para o setor de boot (o grupo de instruções que o computador lê do disco quando é ligado). Já tiveram o seu auge da fama, mas hoje estão se tornando cada vez mais raros.

Vírus executáveis

Também conhecidos como vírus de arquivos, estes programas se anexam ao código executável de

outros programas, principalmente os que contém a terminação .EXE ou .COM. Quando um programa infectado é executado, o vírus vai para a memória do computador e de lá infecta outros programas que são executados posteriormente.

Vírus de Macro

Estes vírus atacam os documentos de gabarito (templates) do Microsoft Office, principalmente o arquivo *normal.dot*. A partir desta contaminação, todo documento criado possuirá o vírus dentro dele, e esta é uma razão pela qual esta categoria de vírus é a mais difundida atualmente. A outra razão é o fato de ser muito mais fácil programar em VBA (Visual Basic for Applications, linguagem de macro do Office) do que em linguagens como Assembler ou C++, utilizada pelos programadores de vírus executáveis.

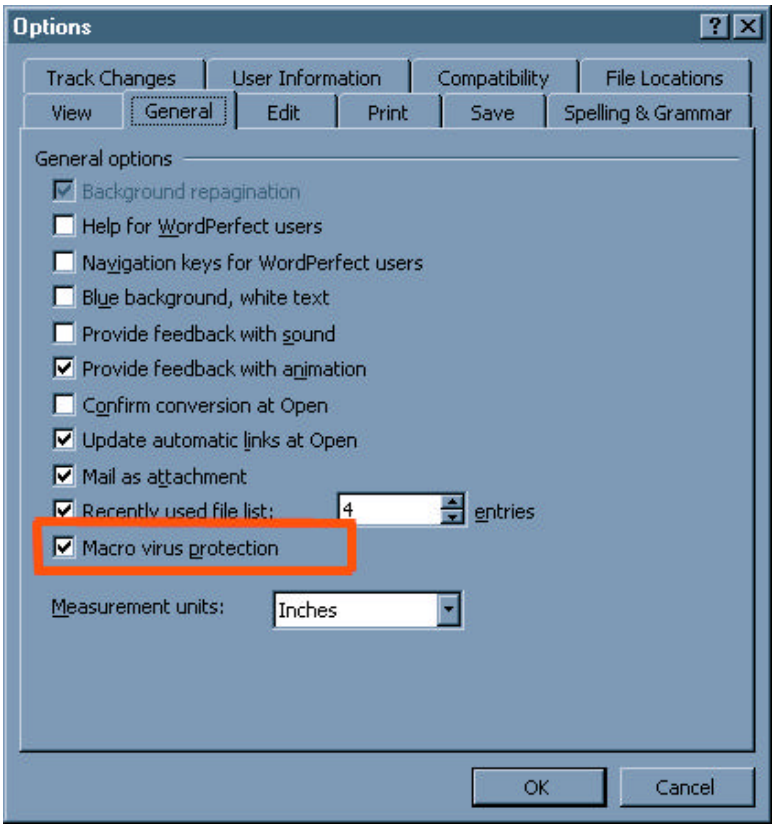

Figura 04_01 – Habilitando a proteção contra virus

Uma boa estratégia de segurança é manter a opção de proteção contra virus habilitada no Word. Esta opção está disponível no menu **Tools|Options|General|Macro Virus Protection**. Assim, sempre que algum arquivo contendo macros for aberto, existirá uma opção que desabilitará o seu carregamento.

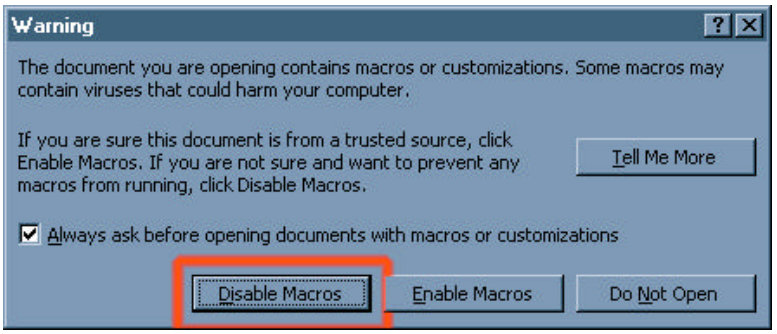

Figura 04_02 – Desabilitando o carregamento das macros no documento Word

Mentiras a respeito dos vírus

Atualmente existe uma histeria coletiva a respeito dos vírus de computador. A cada nova mensagem relatando um novo vírus, praticamente toda a população que está conectada troca mensagens alertando, e por incrível que pareça a grande maioria não passa de mensagens falsas (chamadas na Internet de Hoax). Este efeito faz com que as pessoas passem a receber a mensagem até dezenas de vezes, durante anos...

Entre estas mensagens, algumas se tornaram famosas:

Good Times

A mais antiga e famosa destas mentiras (circula desde 1994), tendo gerado dezenas de filhotes.

Ebola

Esta mensagem circulou impunemente durante vários meses, assustando milhares de pessoas em todo o mundo

MP3

Uma interessante mensagem que levou muita gente a apagar seus arquivos MP3. Veja a mensagem a seguir:

Instituto descobre virus MPEG

Pesquisadores do Instituto IWA anunciaram a descoberta do promeiro vírus de computador multi-aplicação capaz de infectar arquivos no formato MPEG Layer 3, mais conhecidos como MP3. O vírus, chamado de Bloat, se aloja na parte executável destes arquivos, afetando os programas executáveis, como o WinAmp, NAD, MusicMatch, RealJukebox e Microsoft MediaPlayer, nos ambientes Windows 3.x,

95, 98 e NT. Sistemas baseados em Unix e MacIntosh aparentemente não são afetados.

O vírus Bloat se espalha de forma similar aos virus de Macro, que afetam os documentos do Microsoft Office. O código do virus é anexado e se espalha em arquivos de extensão mp3, no momento de sua execução pelo player. O virus anexa uma string de dados após a área reservada para o título e nome do artista, no próprio arquivo mp3. Arquivos similares de áudio, como VQF, WAV, RA e AAC não são passíveis de infecção.

Maiores informações sobre o vírus Bloat e softwares de detecção e limpeza estão disponíveis no site do Instituto IWA, localizado no endereço http://www.iwa.com.

Não há razão para pânico

De fato, dos milhares de vírus já catalogados, somente uns 500 estariam se espalhando pelos computadores, e a maioria deles não contém maiores sofisticações na parte técnica. Aliado ao uso de um software anti-vírus, a possibilidade de eliminação do vírus é elevadíssima.

Estariam nossas máquinas perfeitamente seguras? Na verdade, se você faz download de programas, acessa arquivos de outras pessoas, insere disquetes no seu computador ou lê mensagens de correio eletrônico, com certeza você tem uma boa probabilidade de se ver cara a cara com um destes “micróbios eletrônicos”.

Evitando os vírus

Embora as mensagens falsas cheguem a levar realmente as pessoas ao pânico, o método de contaminação não é tão sofisticado assim. Por exemplo, e até o momento, o ato de se abrir uma mensagem não é capaz de contaminar ninguém. No entanto, se a mensagem contém arquivos anexados, todo cuidado é pouco. Não rode arquivos executáveis e de documentos anexados sem antes passar um anti-vírus atualizado nele. Além disso, não é possível pegar um vírus simplesmente navegando na Internet. Tanto o Netscape Navigator quanto o Internet Explorer já tiveram (e possivelmente ainda têm) falhas de segurança, mas estas falhas são rapidamente sanadas pelos fabricantes. Logo, uma boa política é sempre utilizar uma versão atualizada

dos browsers. E sempre que for fazer o download de um arquivo, passe imediatamente um anti-vírus antes de abri-lo ou executá-lo.

Os melhores programas anti-vírus

Embora existam dezenas de programas anti-vírus, dois são os preferidos dos usuários no mundo todo: o Symantec Norton Anti-vírus e o Network Associates McAfee Viruscan.

O NAV

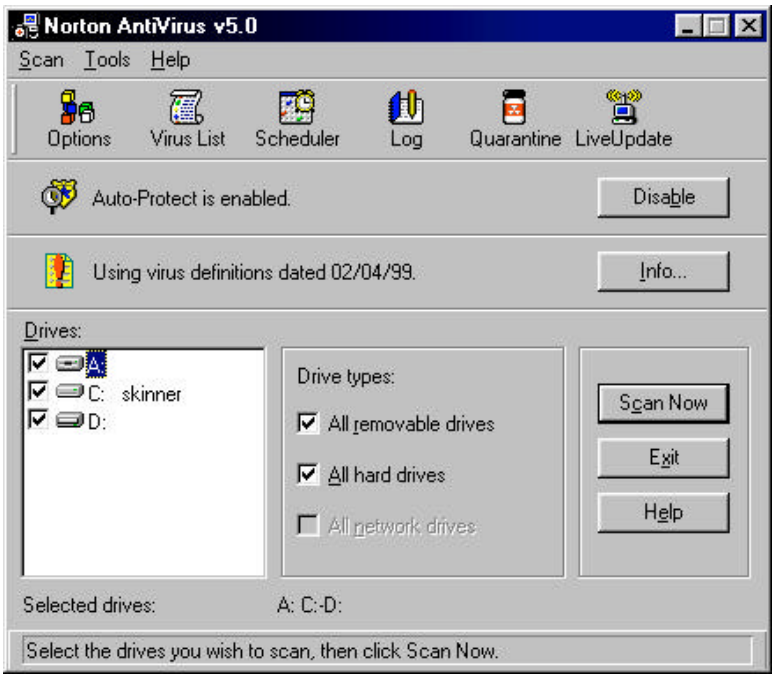

figura 04_03 – O Norton Anti-virus

O Norton Anti-vírus 5.0 é um dos mais poderosos e inteligentes softwares anti-vírus do mundo. Possui uma série de recursos de última geração, como a possibilidade de se colocar arquivos suspeitos em quarentena, e protege também seu computador contra código ActiveX e applets Java malignos.

Outro recurso interessante é o chamado LiveUpdate, que é a atualização de sua base de dados automaticamente, fazendo com que se tenha sempre a última versão das definições de vírus.

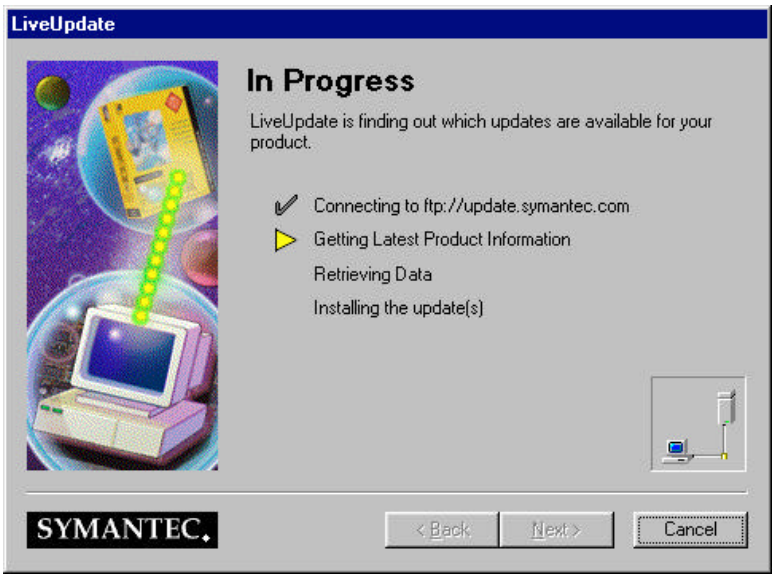

figura 04_04 – O Live Update sendo executado

Outra característica inédita é a possibilidade de se enviar diretamente os arquivos suspeitos para o Centro de Pesquisas da Symantec, através da Internet.

Uma versão de avaliação do Norton Anti-vírus pode ser obtida no endereço http://www.symantec.com/region/br/product/nav/fs_nav5-95nt.html

O Víruscan

O Víruscan é um veterano na área de anti-vírus e agora conta com um aliado adicional: com a compra de outro veterano, o Dr. Salomon, a McAfee introduziu novas formas de detecção e limpeza de arquivos infectados, tornando um excelente produto ainda melhor.

figura 04_05 – O Viruscan

Um recurso interessante é o ScreenScan, que automaticamente inicia o processo de rastreamento de vírus sempre que o Screen Saver do Windows é iniciado.

O Viruscan (versão de demonstração) pode ser obtido no endereço http://www.mcafee.com/centers/download/.

Capítulo 5

Criptografia

Protegendo os seus dados

As suas mensagens de correio eletrônico trafegam abertamente pela Internet e passam por dois ou mais computadores até chegarem ao destino final. No meio do caminho é muito fácil alguém interceptá-las e ler (até mesmo alterar) o seu conteúdo, sem que ambas as partes percebam.

Imagine o estrago que isso pode causar se você, por exemplo, faz uma compra pela Internet e envia o número do seu cartão de crédito por email? Ou se você deseja ter uma conversa em particular com um amigo/amiga distante e não quer que mais ninguém saiba o que vocês estão discutindo? A solução acima é a mesma apresentada para a segurança em redes locais: a criptografia.

Diz a lenda que a primeira aplicação de criptografia foi inventada pelo imperador romano Julio César, que enviava mensagens aos seus generais trocando

letras do alfabeto a partir da regra “pule três”. Através deste esquema, as letras eram trocadas pela terceira letra seguinte no alfabeto. Desta forma, somente quem soubesse da regra conseguia desfazer o algoritmo e ler a mensagem original.

Uma mensagem criptografada só pode ser aberta por aqueles que sabem a senha. Utilizando um programa especial, você pode proteger uma mensagem com uma senha, e a pessoa do outro lado, poderá abrir a mensagem utilizando esta mesma senha. Dois programas para este tipo de tarefa são o ControlMail, disponível em http://www.controlmail.com/, e o Codex, disponível em http://jump.to/icb.

Esta forma tradicional de criptografia, chamada de criptografia de chave secreta ou de chave simética, é bem rápida e eficaz quando não se tem que enviar dados para um número muito grande de destinatários.

O problema é que neste esquema ambas as partes têm que concordar em uma senha. Se o destinatário não conhece a senha, você tem que enviá-la de

alguma forma, e aí caimos em um dilema. A mensagem que estamos enviando com a senha pode ser interceptada e o seu canal de comunicações que aparentemente era seguro, passou a ser quase tão aberto, pelo menos para as pessoas que sabem a senha, quanto mensagens normais!

Uma das soluções para esse problema foi resolvida com a chamada Criptografia de Chave Pública, ou Criptografia Assimétrica, inventada por Whitfield Diffie e Martin Hellman em 1975.

A idéia básica é a seguinte: cada usuário tem uma chave pública, que é distribuida para os outros, e uma chave privada que não pode ser descoberta. As chaves pública e privadas são ligadas através de um poderoso algoritmo, e a idéia básica é a utilização da chave pública de um usuário para enviar mensagens criptografadas para ele. Como as chaves são intrinsecamente ligadas, somente este usuário, ao receber a mensagem criptografada, possuirá a sua chave privada correspondente e poderá descriptografar a mensagem.

Com a utilização deste esquema, acaba-se com o problema de gerenciamento de senhas, já que o usuário somente terá que se preocupar com a sua chave privada. As chaves públicas são distribuídas livremente e inclusive podem ser publicadas em servidores abertos.

Um dos melhores programas, e de longe o mais popular, para esse tipo de criptografia é o PGP, que em sua versão internacional está disponível para download no endereço http://www.pgpi.com/.

Gerando seu par de chaves

Para instalar o PGP, basta clicar duplamente no arquivo de instalação **Setup.exe**, após a abertura do pacote que você obteve no site do PGP. Após a instalação, o primeiro passo a ser realizado é a geração das suas chaves pública e privada. Este procedimento, que é feito através de um assistente (Wizard), será detalhado a seguir.

Inicialmente, acesse a opção **Start|Programs|PGP|PGPkeys**. Será aberto o Assistente de Geração de Chaves.

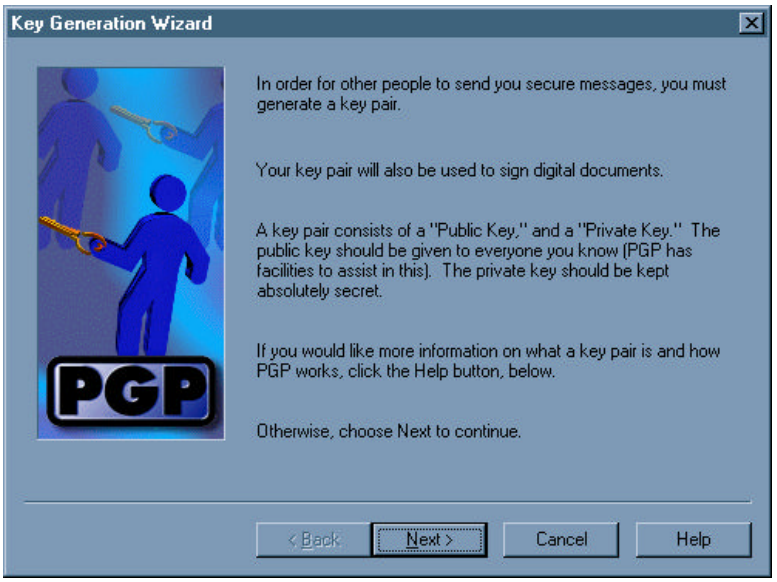

Figura 05_01 – O Assistente de Geração de Chaves

O passo seguinte requer alguns dados pessoais, como nome e endereço de correio eletrônico.

Figura 05_02 – Entrando com seus dados pessoais

Em seguida, escolha o algoritmo a ser utilizado pelo PGP. Embora a opção RSA seja mais universal, o algoritmo Diffie-Hellman/DSS é considerado mais seguro.

Figura 05_03 – Escolhendo o algoritmo

A escolha do tamanho da chave é o passo a seguir. Em geral, quanto maior a chave maior a segurança, mas isso acarreta em perda de desempenho. Uma chave de 2048 bits costuma ser suficiente para a maioria das aplicações.

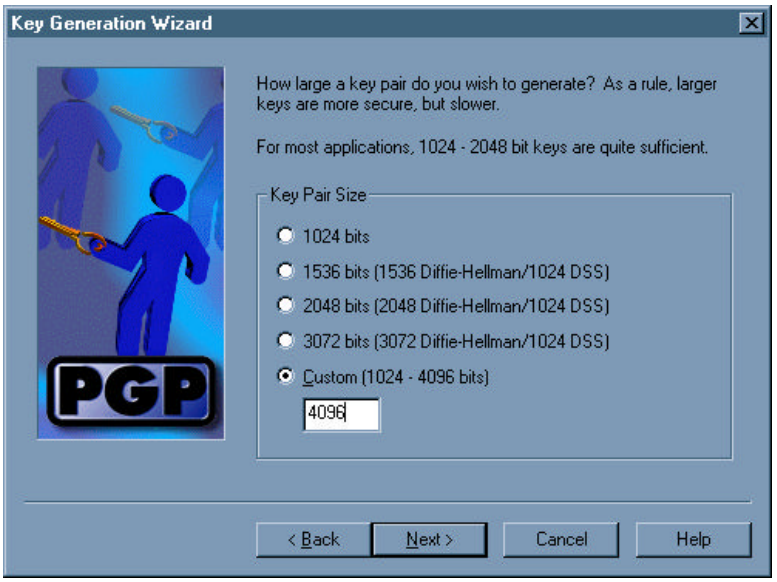

Figura 05_04 – Escolhendo o tamanho da chave

Na sequência, devemos determinar se nossas chaves terão ou não validade determinada. Em geral, é uma boa política selecionar um período de tempo determinado para a validade da chave.

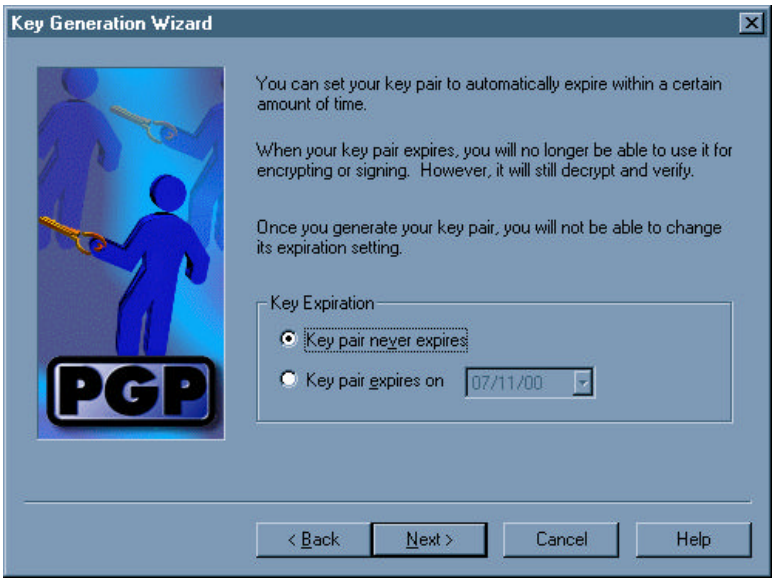

Figura 05_05 – Determinando a validade da chave

Devemos neste ponto escolher nossa frase-senha, que será a chave de acesso à nossa chave privada. Não podemos esquecer que a chave privada, embora não seja distribuída para ninguém, fica fisicamente armazenada em nosso computador, e isso não impede que alguém a acesse. Para evitar este tipo de "ataque" é que existe a frase-senha, que deverá ser alfa-numérica e com pelo menos 8 caracteres. Uma régua mostra a qualidade da combinação escolhida. Em geral, palavras que não se encontram no dicionário são mais difíceis de serem quebradas por hackers.

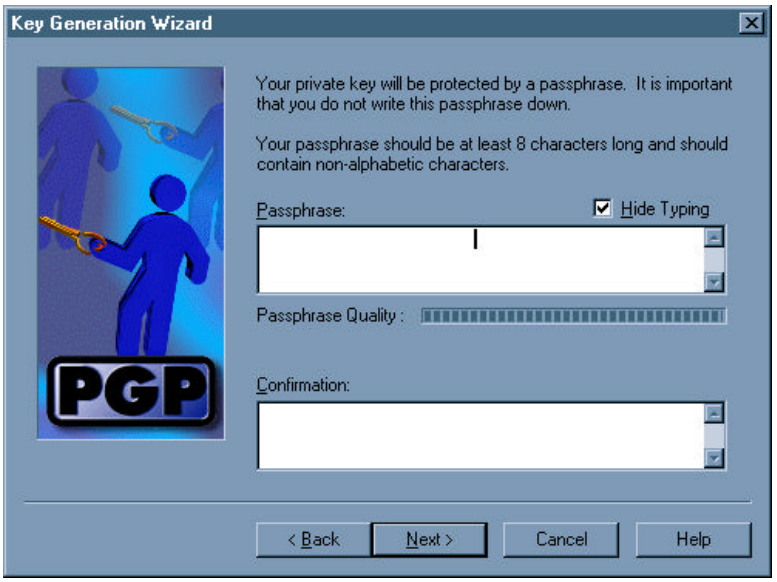

Figura 05_06 – Escolhendo a frase-senha

Em seguida, o par de chaves será gerado e após clicar no botão Next, podemos determinar se nossa chave pública será enviada para um servidor de chaves, localizado no site da Network Associates.

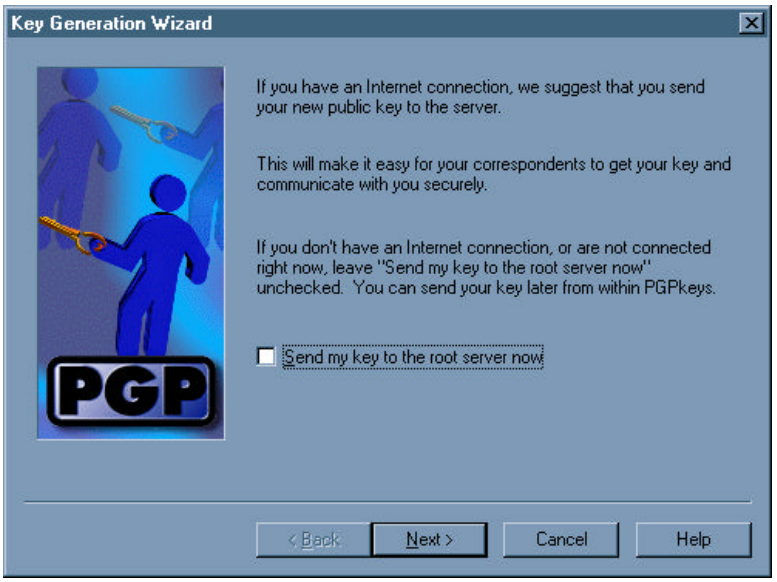

Figura 05_07 – Enviando sua chave pública para o servidor da NAI

O processo estará terminado após você clicar no botão **Finish**.

Criptografando um arquivo

Acesse inicialmente o Windows Explorer e selecione o arquivo a ser criptografado. Em seguida, clique com o botão direito do mouse e escolha a opção **PGP|Encrypt**.

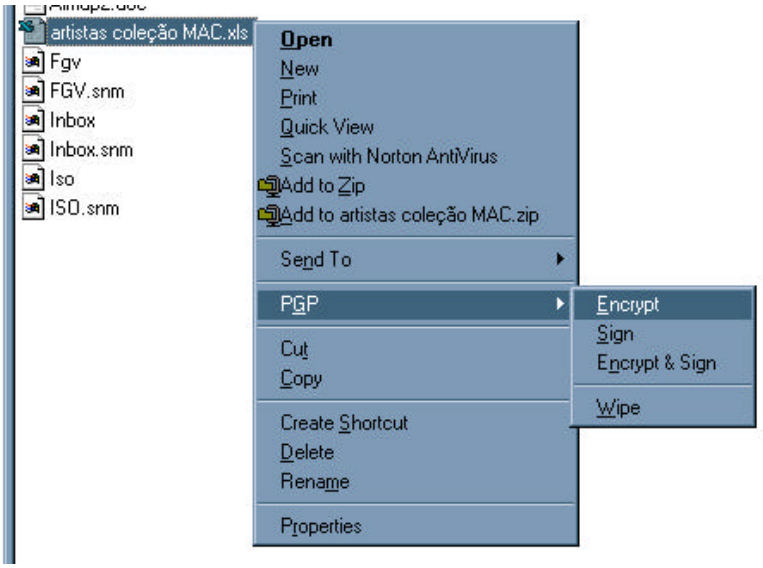

Figura 05_08 – Selecionando a opção Encrypt

Será aberto o menu de criptografia do PGP. Você deverá selecionar em seguida, o nome do usuário (clicando duplamente no seu nome) para quem o arquivo será enviado. Na verdade, neste ponto você estará escolhendo a chave pública do destinatário.

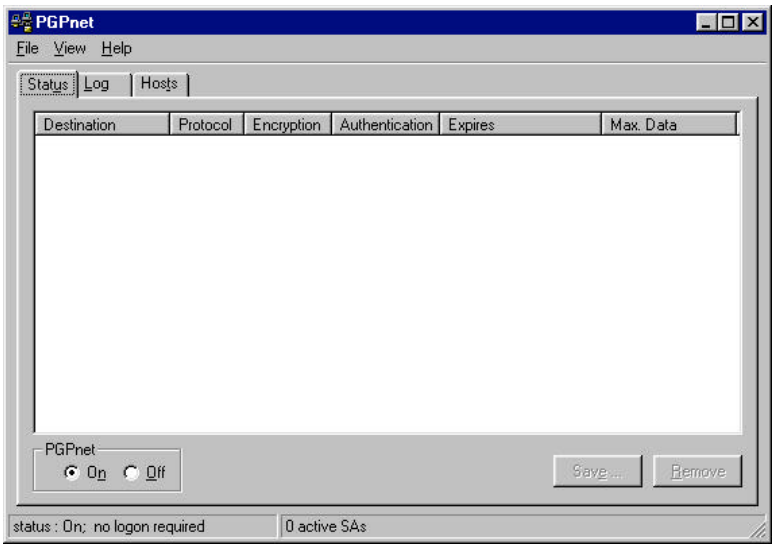

Figura 05_09 – Selecionando o destinatário do arquivo

Basta clicar em **OK** para finalizar o processo. O arquivo criptografado terá a extensão .pgp e poderá ser enviado para o nosso destinatário, através do anexo de uma mensagem de correio eletrônico.

Criando uma VPN com o PGP

Caso você não confie nos usuários de sua rede, a solução é criar uma VPN (Virtual Private Network). Este termo atualmente engloba vários significados. Um deles é o da rede *internamente segura*, utilizando o protocolo IPSec. Desta maneira, todas as

transmissões de dados entre dois computadores são criptografadas.

Isso não impediria que um intruso capturasse todos os dados de sua rede, mas eles ficariam completamente irreconhecíveis para o criminoso digital.

Um dos programas mais populares de criptografia, o PGP, traz nas suas versões 6.x com uma ferramenta de VPN, chamada PGPnet.

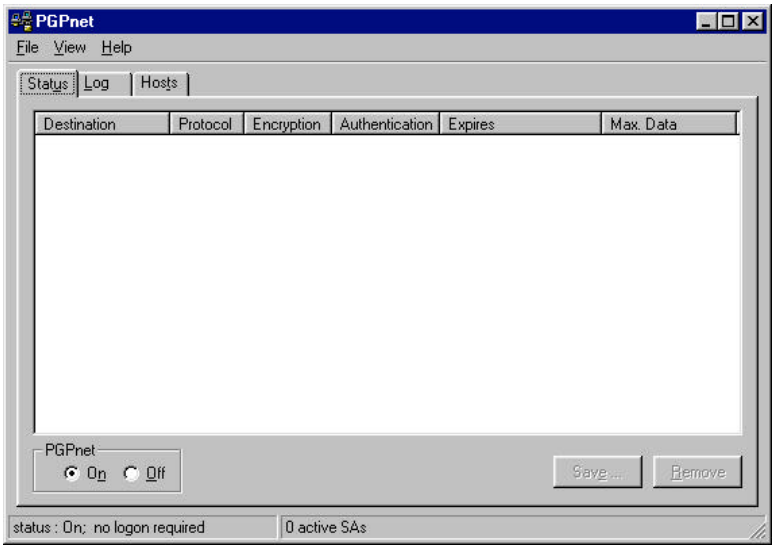

Figura 05_09 – O PGPnet

Basta instalar o PGPnet em todas as máquinas da sua rede, que ela estará relativamente segura.

Capítulo 6

Protegendo-se de Applets Java malignos

Teoricamente, qualquer programa codificado em Java pode ser executado em qualquer computador. Isto é implementado inserindo-se um “processador” Java dentro de cada computador. Este “processador”, que é denominado de Máquina Virtual Java, é um programa que permite a qualquer computador emular um “processador Java” ideal e padronizado.

A Máquina Virtual executa os programas Java interpretando os seus comandos, um a um, e desta forma comandando o computador para que este execute todas as tarefas necessárias ao funcionamento do programa Java. Este esquema é similar a uma emulação, mas suas vantagens são significativas, como o tamanho compacto dos programas, a impossibilidade teórica da proliferação de virus e a possibilidade de computadores até então incompatíveis executarem exatamente o mesmo software.

Como o Java foi feito para ser utilizado em ambientes interconectados, foi dada muita ênfase à segurança. O Java permite a construção de sistemas livres de virus e de falsificações. A técnica de autenticação é baseada em criptografia de chave-pública.

Outra vantagem do Java é possuir uma extensa biblioteca de rotinas para copiar facilmente com protocolos TCP/IP, como HTTP e FTP. As aplicações em Java podem abrir e acessar objetos através da rede via URLs com a mesma facilidade que programadores estão acostumados quando acessam um arquivo do sistema local.

O Java foi projetado para suportar aplicações em rede. Em geral, as redes são compostas de uma variedade de sistemas, com diferentes arquiteturas de sistema operacional e CPUs. Para permitir que uma aplicação Java seja executada em qualquer ponto da rede, o compilador gera um formato de arquivo do objeto de arquitetura neutra - o codigo compilado é executável em muitos processadores, dada a presença do sistema runtime do Java.

Esta característica é útil não só para redes, mas também para distribuição de software de sistema único. No mercado atual de computadores pessoais, os fabricantes de software têm que produzir versões compatíveis com o PC e com o Macintosh. Com novas plataformas e sistemas operacionais, torna-se quase impossível a produção de softwares que rodem sobre todas as plataformas. Com o Java, a mesma versão do aplicativo roda sobre todas as plataformas.

O compilador Java consegue isso gerando instruções de código byte (bytecode) que não tem nada a ver com uma arquitetura de computador em particular. Mais do que isso, as instruções são projetadas para serem tanto fáceis de interpretar em qualquer máquina quanto facilmente traduzida no código da máquina nativa instantaneamente. O interpretador Java pode assim executar bytecodes Java diretamente em qualquer máquina para qual tenha sido transferido.

No entanto, todas essas características também podem ser integradas em browsers, através de

programas auxiliares ou plug-ins. O que faria o Java uma coisa especial?

O Java é uma linguagem de programação para aplicações distribuídas. Ele não somente permite adicionar novos tipos de conteúdos às páginas, permitindo a adição dos dados e do código necessário para visualizá-lo. Desta forma, não é necessário esperar um novo release para o tratamento das informações a respeito do conteúdo.

Esta importante característica do Java é uma autoadequação a novos protocolos, desde que estes sejam escritos em Java. Assim, caso seja desenvolvido um novo protocolo para compressão de audio e vídeo, este protocolo seria carregado assim que uma aplicação o requeresse. A Máquina Virtual Java se atualizaria desta forma, possibilitando sempre a adoção das mais avançadas tecnologias disponíveis na rede.

Além disso, o Java não é utilizada somente em sites Web. O Java é uma linguagem de programação completa, que permite aos seus programadores fazer tudo o que linguagens como o C++ e o Pascal

permitem. Como foi projetada recentemente, teve vários melhoramentos em relação às outras linguagens, sendo considerada também mais simples e intuitiva que outras linguagens anteriores.

Isso foi o que os engenheiros da Sun previram. Parafraseando o genial Garrincha, parece que esqueceram de combinar isso com os adversários…

Sabe-se hoje que já existem uma série de softwares que, utilizando esta sintaxe, agem de forma a prejudicar usuários menos precavidos.

Como o Java nada mais é do que uma linguagem de programação, nada impede que um programa maligno, como um virus, possa ser codificado nesta sintaxe. Programas deste tipo (também chamados de stand alone) podem executar uma série de ações no seu computador, como danificar ou mesmo apagar dados.

Já os applets Java são softwares codificados para serem executados através de um browser, e teoricamente não poderiam comandar diversas ações, como acessar os dados do sistema cliente.

O problema, neste caso, é que o modelo de segurança da sintaxe Java está longe de ser perfeito, e programadores menos escrupulosos podem aproveitar estas brechas para codificar sistemas que podem prejudicar gravemente o sistema do usuário.

Quanto aos controles ActiveX, a situação é pior ainda, já que o seu modelo de segurança é mais frágil ainda, expondo o usuário a riscos ainda maiores do que no caso de applets Java.

Relatos nos mostram que pelo menos um destes códigos malignos já teria a capacidade de transferência de fundos entre sistemas de home-banking baseados no software Quicken.

E para culminar, os softwares de rastreamento de virus tradicionais não têm eficácia nenhuma nestes casos.

Para a defesa contra estas ameaças, estão disponíveis atualmente uma série de softwares de proteção contra ameaças através da rede. Além dos tradicionais anti-virus, estes pacotes oferecem proteção contra sistemas hostis, como applets Java e controles ActiveX.

Entre estes pacotes, um dos softwares mais interessantes é o WebScanX, que utiliza métodos heuríticos e rastreamentos para repelir ataques de controles, applets e sites, sem perda notável de performance em nosso sistema.

Analogamente a um anti-virus convencional, o WebScanX possui uma biblioteca de applets Java e controles ActiveX malignos, bem como uma extensa lista de números IPs e domínios suspeitos. Novas ameaças, identificadas através dos métodos heurísticos (por exemplo, o apagamento de arquivos em determinada sequência), são incluídas na biblioteca de malfeitores.

O WebScanX é capaz até mesmo de suspender o download de arquivos suspeitos, além de interromper o carregamento de applets e controles suspeitos, antes que estes sejam capazes de alguma atitude prejudicial. No momento em que um código maligno está sendo carregado, o usuário é alertado através de uma janela pop-up, e pode desta forma autorizar ou não o seu carregamento.

Capítulo 7

Protegendo-se no IRC

Fazendo chat seguro

Muitas vezes você está no IRC e alguém de for a do canal começa a te enviar dezenas de mensagens, ou sua tela se enche de lixo enviado por alguém que você nunca viu. Eis aqui algumas dicas de como se livrar deste tipo de atitude.

Como o vândalo encontra você

A maioria dos programas IRC permitem que qualquer um procure por nomes no IRC através dos comandos **/names** e **/who**. Se você executa /who #canal, de fora do canal, você recebe uma lista de todas as pessoas no canal. Você pode usar o comando /who *.tal.com.br para descobrir todo mundo do provedor **tal.com.br**. Ou ainda /who *fulano* para encontrar todo mundo que se chama “fulano”.

Tornando-se invisível

Você pode prevenir a maioria das mensagens

indesejáveis tornado-se invisível. O comando para se tornar invisível no IRC é

/mode NICK +i

onde NICK é o seu nickname (ou apelido).

Fazendo-se invisível no IRC significa que apenas aqueles que conhecem o seu nick exato ou que estão no mesmo canal que você é que podem te ver numa procura /who (como mostramos acima).

Para livrar-se de um ataque, fique invisível, e mude de nick. Assim o vândalo não conseguirá mais te encontrar.

/ignore vândalos

Muitos programas de IRC permitem que você bloqueie mensagens de pessoas específicas. No mIRC, por exemplo, você pode entrar com os dados em um menu ou digitar /ignore *!*usuário@*domínio, onde **usuário** e **domínio** são os dados que aparecem na tela quando você digita **/whois nick, como no exemplo:**

/whois linux

linux is ~root@7Dt34YlxUHk.XXXXXXX.com.br * Charlie Root

linux on @#AAAAAAA

linux using PROVEDOR.ORG.BR PROVEDOR – Cidade/Estado

linux is away: is away: (Auto-Away after 10 mins) [BX-MsgLog On]

linux has been idle 18mins 10secs, signed on Tue Nov 02 23:10:26

linux End of /WHOIS list.

O **usuário** no caso é ~root e o **domínio** é 7Dt34YlxUHk.XXXXXXX.com.br. Para ignorar essa pessoa, basta digitar:

/ignore *!*~root@*7Dt34YlxUHk.XXXXXXX.com.br

Combatendo um ataque

Algumas vezes o usuário é inundado de mensagns e comandos CTCP, causando a sua desconexão automática do servidor IRC. Isso é chamado de **flood**. Caso você esteja sofrendo um ataque **flood**, faça o seguinte:

1. Coloque todo mundo temporariamente em **/ignore**, através do comando /ignore *@*.

Ignorando todo mundo você terá tempo de agir antes que uma inundação o desconecte.

2. Fique invisível
3. Mude seu *nick*
4. Descubra o **usuário@domínio** da pessoa que está atacando, normalmente existem vários.
5. Tire o ***/ignore*** para todo mundo, e coloque-o nas pessoas que estão atacando.

Capítulo 8

Segurança no ICQ

Mensagens em cadeia e uma chuva de URLs recebidos em um único dia pelo ICQ nunca foram mais do que um pequeno incômodo. Depois que a febre do ICQ se espalhou, os ataques foram ficando cada vez mais intensos. Aqui iremos listar algumas formas de ataques via ICQ, e como evitá-las.

Bombas / floods

O problema aqui é o mesmo do IRC. Você está conectado à Internet e de repente dezenas, centenas de mensagens começam a aparecer no seu ICQ. Você está sendo bombardeado.

Existem dezenas de programas especializados em causar destruição pelo ICQ. Basta que o seu UIN (o seu número de identificação) seja descoberto para você ser um possível alvo. E a tática utilizada anteriormente no IRC não fará efeito, fazendo com que o programa ignore os UINs que você recebe, pois eles provavelmente são forjados e aleatórios.

Parece sem saída? Nem tanto. Existem maneiras de evitar este tipo de situação, e são soluções bastante simples:

A primeira de todas é a de esconder o número IP da sua máquina. Os piores tipos de ataques são aqueles que são direcionados diretamente para a sua máquina, sem passar para o servidor da Mirabilis. Isso tudo porque o ICQ divulga publicamente, se você permitir, o seu número IP. Para evitar isso, clique no ícone do ICQ, e acesse o menu Preferences and Security e escolha a opção *Security & Privacy*, na parte *Security*, habilitando a opção *Do not publish IP address*.

Figura 08_01 – O menu Security

Outra boa prática é a de apenas aceitar mensagens das pessoas que estão na sua lista de amigos. No mesmo menu *Security & Privacy*, vá na parte Ignore List. Aqui temos algumas opções para seu auxílio:

Figura 08_02 – O menu Ignore List

? **Accept messages only from users on my contact list**

Faz com que o ICQ ignore mensagens de pessoas estranhas a você. Como a maioria das pessoas que podem atacar são estranhas a você, esta é uma boa pedida.

? **Do not accept Multi-Recipient Messages from ...**

Ignore mensagens que foram enviadas para mais de uma pessoa. Você pode ignorar mensagens

originadas de pessoas da sua lista, ou de todas as pessoas em geral.

? **Do not allow direct communication with previous (less secure) client.**

Não permite que você se comunique com versões mais antigas do programa ICQ. Isso é importantíssimo, pois estas versões não respeitam a opção de se esconder o número IP. Mesmo você tenha optado por esta característica, ela será ignorada com verões mais antigas.

Na infelicidade de você sofrer um ataque, existem alguns utilitários que ajudam a remover das mensagens em excesso. Dois deles são o ICQ Bomb Squad, e o ICQ Deflooder, ambos disponíveis em
http://www.arcwebserv.com/jumpsite/icqprotect.html.

Lembre-se sempre: mantenha o seu ICQ atualizado! Versões mais antigas (98, por exemplo) do programa estão sujeitos a ataques tanto quanto as versões mais antigas do Windows, como discutimos acima. Utilizando as técnicas de varredura de portas, é muito fácil encontrar uma máquina rodando o ICQ, já que

ele utiliza portas conhecidas, normalmente numerada entre 1000 e 2000. Lembra-se dos potes de mel? Existem um pote de mel para despistar um ataque. É o ICQ Protector (disponível no mesmo lugar do ICQ Bomb Squad e o ICQ Deflooder), que abre várias portas, fingindo ser o ICQ original. Assim quando alguém varrer as portas do seu computador, você saberá que está sendo farejado.

Capítulo 9

Implementando um firewall pessoal no seu PC

Para se proteger de forma mais definitiva, todos os cuidados vistos anteriormente ainda não são considerados relativamente eficazes contra ataques mais sofisticados.

O ideal é mesmo a instalação de um firewall pessoal no seu computador. Um firewall é um software que filtra todo o tráfego da rede e a torna imune a acessos não autorizados.

Entre dezenas disponíveis no mercado, selecionamos o ConSeal Private Desktop, que possui uma série de recursos para tentar proteger ao máximo o seu sistema.

Disponível em versão de avaliação no endereço http://www.signal9.com, o Private Desktop se mostrou eficaz contra uma série de ataques, como o Back Orifice, Winnuke, jolt, ssping, land, bonk, teardrop,

newtear, boink, tear2, puke, smurf, unreach, ipjolt, spring, icmp flood e o udp flood.

Nota: antes da sua instalação no Windows 95, é necessário instalar o update do Winsock 2.0, disponível no endereço http://www.microsoft.com/windows95/downloads/contents/wuadmintools/s_wunetworkingtools/w95sockets2/default.asp?site=95. O Windows 98 já vem com esta atualização.

Sua instalação é bem simples: basta clicar no arquivo cpd95_v204.exe. Um aplicativo de instalação completará o processo, e após um reboot o software estará pronto para ser utilizado.

A partir da interface com o usuário, podemos configurar uma série de parâmetros responsáveis pela nova política de segurança da sua máquina.

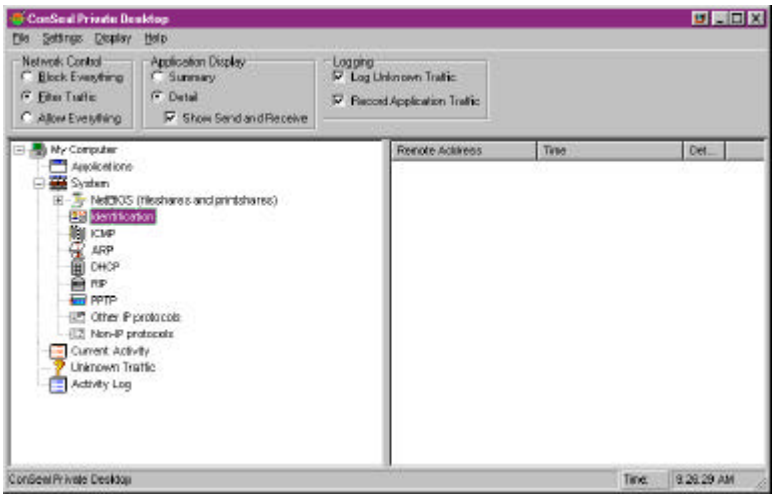

Figura 09_01 – A interface do Private Desktop

O primeiro parâmetro a ser configurado é o painel Network Control, que pode ser configurado para bloquear todo o tráfego da rede (Block Everything) - uma boa iniciativa no caso da máquina estar ociosa, filtrar os pacotes da rede (Filter Traffic) ou permitir o tráfego sem restrições (Allow Everything).

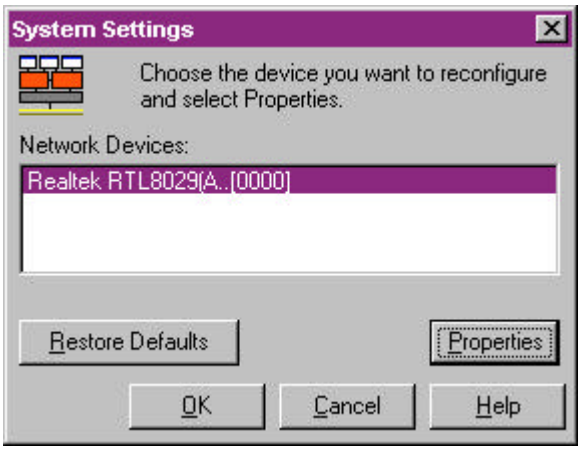

Figura 09_02 – Configurando o sistema

Clicando-se em seguida no menu Settings|System, pode-se configurar o dispositivo de rede utilizado. Normalmente, este dispositivo será ou uma placa de rede (no caso de acesso direto à rede) ou um modem (no caso de acesso discado).

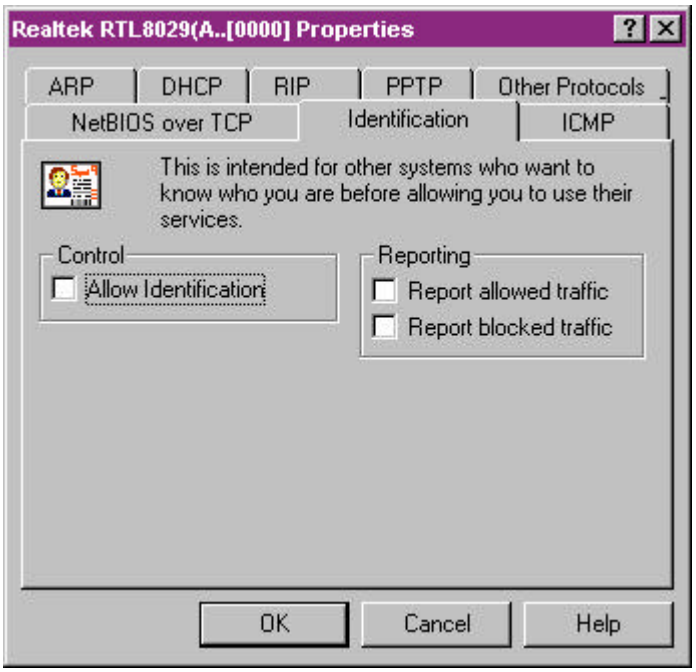

Figura 09_03 – Configurando o dispositivo de acesso à rede

Para acessar o menu de configuração do dispositivo, basta selecionar a opção Properties. Neste menu, é possível bloquear uma série de protocolos e métodos de ataque, bem como desabilitar certas características de identificação utilizadas por hackers para obter informações sobre o seu sistema.

As informações importantes são:

- Na seção Other Protocols, verifique se todos os protocolos listados estão bloqueados (opção Block Incoming Fragments).
- Na seção ICMP, selecione a opção Block all ICMP
- Na seção Identification, desabilite a opção Allow Identification

Com estas providências, podemos ter certeza que nosso sistema estará bem mais seguro do que antes da instalação do Firewall. Mas todo cuidado é pouco, pois os invasores estarão sempre correndo atrás de novas vulnerabilidades.