KIT DE FERRAMENTAS MULTITAREFAS HACKER

PORTSCAN
O papel de um portscan é percorrer todas as portas de um endereço IP especificado, com um intervalo geralmente determinado pelo utilizador. Então é feita uma checagem, a procura de conexões nestas portas, uma a uma, a fim de identificar qual daemon e versão responde por determinada porta.

JAMMER
Com esse programa, ninguém consegue rastrear seu IP.

NETBUSSOFT
Um dos melhores programas cliente/servidor - P2P

ANTI HACKER 2.0
É um dos menores firewall do mercado, mas é muito eficiente.
Monitora o sistema. Programa Totalmente gratuito, sem tempo de uso. For win 95/98.

SUBSEVEN
SubSeven (Sub7) é um programa par invadir computadores de usuários normais, como você, é muito simples de utilizar para quem entende inglês, se você não entender nem um pouco aprenda, ou você não sai do lugar.
Cuidado para não executar o "server.exe", se você executar esse arquivo, poderão invadir seu pc com este programa aí você vira a diversão dos outros invés de se divertir com os outros se isso acontecer, procure um removedor de trojan.

ONTRACK
Varre seus programas em busca de bugs.

NETBUSTERKILLER
Antídoto contra Backorifice, Trojanhorses.

WEBCRAKER
"Crakeie" segredos e páginas da net.

MultiProxy
Freeware. Navegue anônimo na Internet!

FTP COMMANDER
Acesse FTP graficamente através do Windows.

FRESH DIAGNOSE
Freeware. Utilitário que analisa e testa os componentes do seu PC.

PASSWORD AGENT
Free..Arquivador de passwords.

FreeFTP
Freeware. Cliente FTP.

HACKERWACKER
Freeware. Monitore e acesse todos os endereços visitados pelo seu browser.

SPYBLOCKER 4.5
Freeware. Mantenha sua privacidade eliminando os spywares.

ProFTPD
FTP para Unix e suas distribuições.
XP-AntiSpy 3.2 Freeware Bloqueie as atualizações automáticas do WindowsXP.

FOLDERLOCK 1.2
Freeware . Proteja e esconda diretórios, subdiretórios e arquivos.

ZONE ALARM
Freeware. Proteja seu computador contra invasores.

COOL FTP!
Freeware. Cliente FTP fácil de usar.

HACKTEC
Anti-hacker eficiente

FXB
detectar e remover o vírus
W32.Bugbear@mm.

Xô Bobus
Combate trojans.

TDS-2
Mapeamento de IPs.

THE CLEAN
Previna-se contra Backorifice.

LINUX

MUSICMATCH JUKEBOX
Shareware. Crie mp3 e toque músicas de vários formatos.

DOOM
Shareware. Jogue este game clássico no Linux.

COFFEECUP HTML
Shareware. Edite HTML no Linux.

LIMEWIRE
Freeware. Baixe qualquer tipo de arquivo com esse programa peer-to-peer.

SHELL
Freeware. Compartilhe arquivos com essa shell peer-to-peer.

MP3

POCHETTE EXPRESS
Freeware. Imprime capas de CD's, DVD's.

CDex
Freeware. Converte CD-áudio em Mp3 ou Wave.

CDCOVER PRINT
Imprime capas de CD's.

PROCESSU CD PLAYER
Freeware. Reprodutor de CD's digitall.

RAMP
Freeware. Leitor de Mp3's estilo autorádio.

K-JÖFOL 2000 1.0
Freeware. Toque MP3/VQF/ACC/CD com uma interface muito louca.

MP3 2000 STUDIO 1.2
Freeware. Toque, decodifique, equalize e crie CDs com MP3.

WINAMP FULL 2.78C
Freeware. Divirta-se com a versão completa do melhor programa de mp3.

MUSICCITY

MORPHEUS1.33
Freeware. Busque mp3 com esta nova sensação do momento.

SHOUTCAST SERVER1.8.3
Freeware. Transforme seu Winamp em um servidor online de MP3.

MUSICMATCH JUKEBOX 7.00
Freeware. Ripe cds e escute seus MP3.

ATENÇÃO: Esse CD-ROM contém programas que podem danificar se micro.Eles foram incluídos no CD exclusivamente para estudo e conhecimento técnico. Não nos responsabilizamos por uso indevido. O uso destes softwares para prejudicar terceiros é crime, passível de sanções da lei.

PROGRAMAS - SEGREDOS - TÉCNICAS - MUNDO UNDERGROUND

invasão HACKER

Kit de ferramentas multitarefas hacker

SPOOFING
Enganando, derrubando e invadindo

IP's A verdade sobre eles
Seu IP foi realmente rastreado?

SPYWARE
Tudo sobre os pixels espiões

GAMES UNREAL E CONTER STRIKE
Leia sobre estes incríveis jogos

CIBERTERRORISMO
Ninguém está seguro!

VIDA E MORTE DE UM HACKER

MITHNIK
Finalmente o segredo vem à tona

No CD
PortScan
Subserven
Hacktec
The clean
Class
Nicbr
TDS-2
Anti-hacker 2.0

Invasão Hacker nº 01 - R$ 9,90
ISSN 1677-9215

hacker

Editora Escala Ltda.
Av. Profª Ida Kolb, 551 Casa Verde
CEP 02518 000 São Paulo / SP
Telefone: (0XX11) 3966-3166 - Fax.: (0XX11) 3857-9643
Internet: www.escala.com.br
E-mail: escala@escala.com.br
Caixa Postal 16.381
CEP 02599 970 - São Paulo - SP

Presidência: Hercílio de Lourenzi
Vice-presidência: Mário Florêncio Cuesta
Direção Editorial e Marketing: Paulo Afonso de Oliveira
Coordenação: Priscilla Ellen dos Reis
Operação e Logística: Nilson Luiz Festa
Assistente: Leandra Maria Spinelli
Supervisão Editorial: Moacir Francisco Amorim, Priscilla Mara G. Ribeiro e Vera Lúcia P. Morais.
Revisão: Ciro Mioranza e Mª Nazaré S. L. Baracho.
Circulação: Jane Cristina da Silva e Zildete da Silva.
Assistente: Liliane Mendes Portelo
Promoção PDV: Álvaro Ângelo Tomiatti
Atendimento ao leitor: Anne Vilar Adriana Ferreira da Silva, Fernanda Ferreira Alves, Sheila Regina Fidalgo e Vanessa Cristina Vieira.
atendimento@escala.com.br
Fone: (0XX11) 3966-3166

Conselho Editorial: Amélia Pessôa, André Lima, Antônio Cedraz, Carlos Gonçalves, Carlos Mann, César Nemitz, Eddie Van Feu, Fábio Kataoka, Franco de Rosa, João Andrade, João César Muraroto, José Romeu Feixas, Marcos Evandro, Marques Rebello, Moacir Costa, Moacir Torres, Otto Schmidt Junior, Paulo Fernandes, Paulo Paiva, Pricila Del Claro, Renato Rodrigues, Rick Mann, Robson Oliveira, Rosana Braga, Rosely Ribeiro, Sandro Aloisio e Victor Rebelo.
Números atrasados: Através do telefone: (0XX11) 3966-3166 ou www.escala.com.br
Impressão e Acabamento: Oceano Ind. Gráfica 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) 3879-7766.
Disk Banca
Sr. Jornaleiro, a Distribuidora Fernando Chinaglia atenderá os pedidos de números atrasados da Editora Escala enquanto houver estoque.
Assinaturas
Em apoio ao jornaleiro, a Editora Escala não trabalha com assinaturas.
Observação Importante
O estúdio MidWest Visual Designer, que criou, produziu e realizou este projeto tem inteira responsabilidade sobre a originalidade e autenticidade de seu conteúdo.
Filiada à ANER.

Criação e Projeto:
MidWest Visual Design

Diretor: Fausto Kataoka
Editor e Diretor: Fábio Kataoka
Coordenador Editorial e Direção de Arte:
Marcelo Romano
Diagramação
Luciano P. Bolognesi
Coordenador de Produção:
Carlos E. Kataoka
Revisão: Maria Zenólia Almeida
Agradecimentos:
Artigos e Colaboração:
Gustavo Brigatto
Equipe Ultrajovem
Consultoria técnica:
Valeska Bielecki
MidWest Visual Design
Rua Horácio Vergueiro Rudge, 495
São Paulo - SP - CEP 02512-060
Telefax: 11-3951 5214

Hackers são bandidos ou mocinhos?

Filósofo finlandês tenta explicar a diferença entre o bom e mau hacker. Os bons estão com a chamada ética hacker, que seria uma alternativa para a ética protestante e exemplo de um novo pensamento.

Invasões a sites e disseminação de vírus: depois de tantos episódios de vandalismo virtual anunciados quase diariamente pela imprensa, ainda é possível ver os hackers como bons sujeitos?

Para o filósofo finlandês Pekka Himanen em seu livro A Ética dos Hackers e o Espírito da Era da Informação (Editora Campus) a resposta é sim, desde que se entenda exatamente o que ele define como um hacker.

Segundo ele, "originalmente um hacker era uma pessoa para quem a programação era uma paixão e que compartilhava as criações dessa paixão com outros (...) e não um criminoso informático

descreve a ajuda de hackers americanos e holandeses para driblar a censura dos meios de comunicação no Kosovo em 1999 e cita os movimentos de Software Livre e Open Source, criados respectivamente por Richard Stallman e Eric Raymond como provas de que os verdadeiros hackers querem liberdade de informação, e não destruição de dados.

Em: *O que faz o coração de um hacker bater mais rápido, também conhecido como Lei de Linus*, o criador do sistema operacional Linux estabelece três categorias básicas que, segundo ele, atuam como motivadoras: sobrevivência, vida social e diversão.

> a capacidade auto-expansível de processamento e a flexibilidade das novas tecnologias de informação são características essenciais para a mudança que a sociedade tem vivido nos últimos anos,

Mais adiante, Himanen pega emprestada essa categorização de Linus e faz uma comparação pertinente e oportuna com o psicólogo Abraham Maslow, conhecido pelo modelo da pirâmide de necessidades básicas humanas que criou, até hoje muito utilizado, principalmente em propaganda e marketing. As três categorias de Linus podem ser comparadas a outras tantas entre as cinco de Maslow, a saber: necessidades fisiológicas e de segurança (sobrevivência), necessidade de pertencer a um grupo social e ser amado (vida social). Himanen sabe que simplificações são perigosas, mas ele próprio faz esse alerta ao leitor e adverte que a comparação é feita apenas para lançar uma luz sobre as diferenças entre os modelos éticos do protestantismo e dos hackers.

Himanen se detém basicamente nas diferentes maneiras como cada grupo encara os fatores tempo e dinheiro. Enquanto os "protestantes", ou seja, os capitalistas antigos e boa parte dos modernos, ainda se pautam pela velha frase de Benjamin Franklin, "Tempo é dinheiro", trabalhando em longas jornadas diárias para só descansar no domingo (e muitas vezes nem isso), os "hackers", neste caso não só os programadores, mas todos aqueles que vivem do que gostam, fazem do trabalho um prazer.

Por isso podem mesmo trabalhar mais do que os capitalistas tradicionais, mas no tempo que eles definirem, da forma como bem entenderem. A questão de dinheiro (vide as polêmicas envolvendo o Linux e o Software Livre) é mais complicada, mas de modo algum é semelhante ao modelo tradicional.

No posfácio de Castells, o autor de A Sociedade em Rede cria o termo informacionalismo para designar um novo paradigma socioeconômico fundamentado na tecnologia, em contraposição ao tradicional industrialismo da nossa sociedade de fábricas e grandes corporações. Através de uma breve biografia da Rede, o sociólogo espanhol explica que a capacidade auto-expansível de processamento e a flexibilidade das novas tecnologias de informação são características essenciais para a mudança que a sociedade tem vivido nos últimos anos, e conclui que o estudo da cultura hacker e o espírito do informacionalismo, que só agora começam a ser estudados de verdade, constituem um avanço fundamental para o mundo neste momento de incerteza. Himanen tem um site dedicado ao tema, mas seu conteúdo se restringe praticamente a uma reprodução de fragmentos do livro.

A parte mais interessante acaba sendo a página de links, que remete o usuário a ótimos sites citados no livro, como os Cypherpunks, grupo que luta pela privacidade de dados através de melhores métodos de encriptação, a Electronic Frontier Foundation, entidade que luta pela liberdade de expressão na Rede e a Free Software Foundation, criada por Richard Stallman para defender a liberdade de uso do software. No entanto, até nas indicações bibliográficas o livro é melhor que o site: paradoxalmente, na obra em papel você encontrará mais endereços de sites para visitar, como por exemplo o sempre atual ensaio de Eric Raymond, The Cathedral and the Bazaar.

Fácil de ler e de compreender, A Ética dos Hackers não é um livro de filosofia, sociologia ou política, pelo menos não no sentido estereotipado ao qual infelizmente ainda estamos tão (mal) acostumados.

Este é um livro sobre a nossa sociedade. Hoje.

Windows polêmica e processo

Um dia após a Microsoft ter lançado a mais recente versão do seu sistema operativo foi divulgada uma nova alternativa designada Lindows

Um dia após a Microsoft ter lançado a mais recente versão do seu sistema operativo foi divulgada uma nova alternativa designada Lindows, liderada por Michael Robertson, fundador e ex-director executivo do serviço de música online MP3.com. O Lindows consiste numa distribuição do Linux que promete funcionar com todos os programas do Windows, da mesma maneira que correriam no Windows 98, NT ou XP.

Segundo Robertson, citado pela Wired, o sistema operativo open-source não conseguiu atrair os utilizadores do Windows devido aos seus hábitos entranhados. Os adeptos da plataforma da gigante de software são relutantes em deixar de utilizar aplicações como o Microsoft Office, mesmo se surgirem alternativas viáveis como o StarOffice da Sun.

De acordo com o comunicado da Lindows, empresa que está por detrás deste projecto, o seu sistema operativo vai funcionar sem problemas num ambiente informático diversificado e irá suportar as impressoras, servidores de ficheiros e de correio electrónico, bem como diverso hardware actualmente disponível no mercado.

De forma a alcançar essa compatibilidade com o Windows, o Lindows utiliza partes do Wine, um emulador do sistema operativo da Microsoft para plataformas descendentes do Unix - como o Linux, FreeBSD e Solaris - que vem sendo desenvolvido desde 1993. Mas segundo Robertson, o Wine é apenas uma parte da área total de compatibilidade do Lindows. O restante do software será desenvolvido pelos próprios programadores da companhia.

Robertson afirmou que espera que o Lindows alcance a total compatibilidade com o Windows dentro de um período de 18 a 24 meses. Na sua opinião, o processo não vai infringir o código-fonte ou direitos de autor da Microsoft.

O problema é que, sendo o Lindows basicamente uma instalação completa do Linux, os utilizadores terão que reformatar os seus discos rígidos e reinstalar todas as suas aplicações. Outro aspecto que poderá dificultar o sucesso do projecto de Michael Robertson é a área de compatibilidade. A Sun desenvolveu um emulador para o Windows designado de Wabi, que foi descontinuado em 1997.

LINDOWS VS WINDOWS

Lindows vs Microsoft [documentos de defesa]

O director executivo da Lindows.com, Michael Robertson - publicou no site da empresa uma carta em que refere os principais pontos da defesa contra a acusação da Microsoft de que está start-up está violando a sua marca registada "Windows" ao utilizar os termos "LindowsOS" e "Lindows.com" para descrever o software que está desenvolvendo, uma distribuição do Linux compatível com programas criados para o sistema operativo da Microsoft.

Os documentos legais de defesa da Lindows.com foram entregues oficialmente no dia 28 de janeiro de 2002 ao Tribunal distrital de Seattle, nos Estados Unidos, estando também disponíveis no site da compania. A empresa vai voltar a defrontar-se com a gigante de software no tribunal a 27 de fevereiro de 2002.

A estratégia principal de contra-ataque da Lindows.com consiste em alegar que a Microsoft está incorretamente tentando impedir que um produto concorrente que rima com a palavra "windows" seja lançado no mercado, justificando que os termos Lindows infringem injustamente a sua marca registada de sistema operativo.

Robertson afirma que "windows" é um termo tão genérico que nenhuma companhia deveria ter o direito absoluto a ele, já que o seu significado na indústria informática é anterior à utilização da Microsoft. "Empresas como a Xerox, DEC, Apple utilizaram-no durante anos para designar os interfaces gráficos de utilizador que incorporam elementos gráficos para exibirem e manipularem aplicações", refere o director executivo. Segundo Robertson, a empresa de Bill Gates só começou a empregar o termo "windows" - referindo-se a um sistema operativo - a partir de 1983.

Outra carta entregue pela Lindows.com na sua defesa é o fato de a Microsoft ter sido acusada de exercer práticas monopolistas: "Independentemente do dinheiro que uma empresa gasta, esta não deve ser permitida de impedir os outros de utilizarem um termo descritivo bastante utilizado na indústria; especialmente se essa companhia foi considerada culpada de efetuar práticas ilegais para construir e manter o seu monopólio".

Uma das testemunhas a que a Lindows.com recorreu para desacreditar a posição da Microsoft foi John Dvorak, jornalista informático há mais de 20 anos, que aproveitou para relembrar que a gigante de software tem o hábito de juntar o seu nome a uma palavra genérica, como "Microsoft Word". A start-up também tentou demonstrar que a Microsoft está tentando paralizar a concorrência ao notar que existem centenas de produtos informáticos com a palavra "windows" ligada a eles. Robertson salientou que a empresa de Bill Gates nunca tentou processar as fabricantes desses produtos.

"Por que é que a Microsoft iria permitir que milhares de produtos utilizassem o que afirma ser a sua marca registada sem qualquer tipo de protesto, mas decidiu processar a Lindows.com?" questiona o documento.

"O fato de a Microsoft estar apenas tentando atingir a Lindows.com demonstra que a sua verdadeira motivação é travar uma potencial concorrente e não que acreditam que existe confusão em relação ao nome do produto."

Para provar que não existe qualquer confusão por parte dos consumidores entre as duas plataformas, a start-up encomendou a uma empresa independente de estudos de mercado um inquérito envolvendo 14 mil potenciais compradores.

O estudo conclui que nenhum dos inquiridos afirmou que Lindows poderia ser um produto lançado pela Microsoft.

Por ultimo, Robertson afirma que a sua empresa disponibilizou à Microsoft uma possível solução de compromisso em que a Lindows.com continuar utilizando o seu nome empresarial mas que, em troca, deixaria de empregar o termo LindowsOS para designar o seu sistema operativo, mas que a gigante de software recusou a oferta. Enquanto isto, a versão de amostra da distribuição do Linux já foi disponibilizada a um grupo seleccionado de programadores.

Primeira versão beta do Lindows será lançada no final do ano

Foi lançada a versão 2.0 do Lindows. Entre as novidades, está a habilidade de se conectar em rede com computadores que usam Windows, visualizando e modificando arquivos.
O software, que promete ser uma espécie de Linux que roda a maioria dos programas Windows, vem se tornando cada vez mais popular e sendo considerado uma alternativa (mais barata) ao sistema operacional da Microsoft.
A idéia foi de Michael Robertson, fundador do MP3.com e criador da nova empresa.
O programa foi construído com base no núcleo Linux e vai rodar os aplicativos mais populares das duas plataformas;suporta diversos softwares da Microsoft como a suíte Office e qualquer programa desenvolvido para o sistema Linux.
O Lindows será um sistema mais parecido com o sistema de Microsoft, em que o uso será bem mais fácil. Qualquer um poderá se beneficiar utilizando o Lindows, estudantes, pequenas empresas e usuários domésticos.
É um sistema voltado única e exclusivamente para desktops e não para servidores como é o caso do Linux.
Para ter maiores informações sobre esse sistema que tanto promete, entre em www.lindows.com

MICROPROCESSADOR

GigaHertz, já é passado

TERAHERTZ

um teraHertz é igual a um milhão de Mhz

Quem pode imaginar um intervalo de tempo de um trilionésimo de segundo?

Com certeza, nossas percepções não conseguem alcançar tal fração de tempo.

É justamente isso que promete a nova tecnologia dos transistores, os chamados TeraHertz. Ela permitirá a construção de microprocessadores muito mais velozes, na marca de um trilhão de ciclos por segundo! Essa nova tecnologia permitirá o surgimento de aplicações avançadas, como reconhecimento facial e computadores do tamanho de relógios de pulso, além de resolver problemas de gasto de energia e aquecimento. Agora, o que limitará a performance do transistor será o consumo de energia, e não a velocidade ou tamanho.

O processador Pentium 4, um dos mais conhecidos e poderosos da atualidade, tem cerca de 42 milhões de transistores. Baseados nessa nova tecnologia, processadores com um bilhão desses componentes devem surgir daqui a alguns anos. Uma grande melhoria foi o desenvolvimento de um novo material. O novo método consiste em revestir as lâminas de silício monocristalino por moléculas orgânicas. O revestimento contém, na verdade, fileiras de

Ela permitirá a construção de microprocessadores muito mais velozes, na marca de um trilhão de ciclos por segundo!

comutadores moleculares que atuam com precisão atômica. Trabalhando em conjunto, esses comutadores permitirão a produção de chips com velocidades de processamento de até 100 terahertz, ou seja, 100 trilhões de instruções por segundo, estes valores são quase inimagináveis, mas já fazem parte de uma realidade muito próxima, o processamento teraHertz.

História em um segundo

No dia 1º de julho de 1948, foi apresentado ao mundo o primeiro transistor, um substituto da válvula eletrônica de três pólos, nos rádios e nos sistemas de telecomunicações. Vale lembrar que nenhum avanço tecnológico produziu maior impacto na vida humana no século XX do que sua invenção. Na verdade, a eletrônica moderna nasce com a válvula, inventada por LeeDeForest, em 1906. Com ela surgiram, durante a primeira metade do século, as comunicações sem fio, o rádio, a televisão, o som de alta fidelidade e os primeiros computadores.

Mas em 1948, foi o transistor que fez o mundo enxergar novos horizontes. O novo componente trazia, no mínimo, cinco exorbitantes vantagens : miniaturização, drástica redução de custo, baixo consumo de energia, longa durabilidade e alta confiabilidade. É tudo que se pode querer em avanço revolucionário.

Logo em seu lançamento, o transistor já é 200 vezes menor do que uma válvula eletrônica. Seu custo, dez vezes menor. Em 1964, nasce o circuito integrado, reunindo numa placa todos os componentes miniaturizados, tais como diodos, capacitores, resistores, indutores e outros.

Em 1971, Robert Noyce lança o primeiro microprocessador, ou seja, a primeira unidade de processamento central ou CPU, tornando viável o nascimento dos microcomputadores. Noyce funda a Intel, a empresa que lançará os microprocessadores mais populares (desde o 8008 até o conhecido Pentium 4).

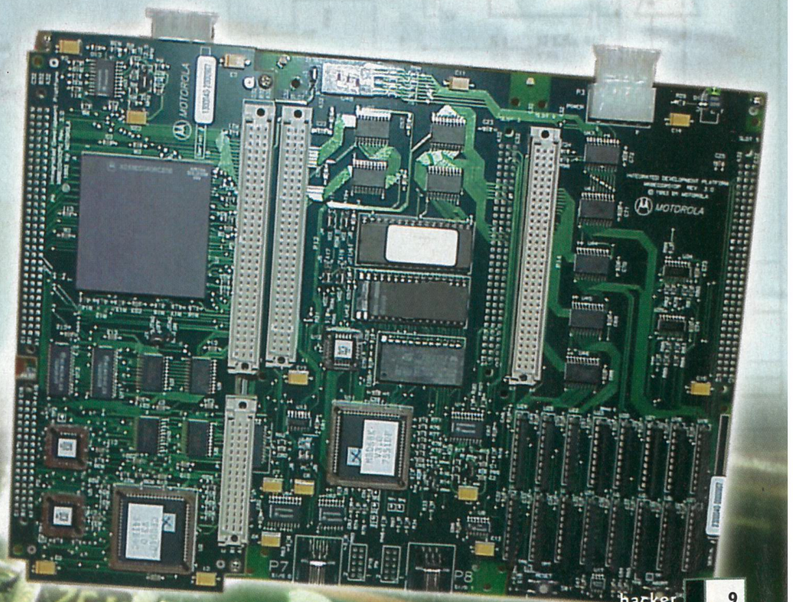
Um companheiro de Noyce, Gordon Moore, formulou o que chamamos de "lei de Moore", segundo a qual o número de componentes dos chips dobra a cada dois anos. Para surpresa do mundo, a lei de Moore vinha sendo rigorosamente comprovada na prática, até agora. Mas com o TeraHertz, a "lei de Moore" poderá ser modificada.

A revolução industrial da microeletrônica tem sido responsável pelo crescimento explosivo da informática, das telecomunicações e da eletrônica de consumo, expandindo-se à incrível taxa média anual de 15,6% por mais de duas décadas. Assim podemos entender melhor o sucesso de algumas corporações gigantes da área, tais como: Intel, Motorola, NEC, Alcatel, IBM, Siemens etc.

O processador Pentium 4, um dos mais conhecidos e poderosos da atualidade, tem cerca de 42 milhões de transistores. Baseados nessa nova tecnologia, processadores com um bilhão desses componentes devem surgir daqui a alguns anos.

Com essas tendências, teremos chips com bilhões de componentes em menos de cinco anos. No mesmo período, todas as funções de um televisor poderão estar armazenadas num único chip. A velocidade de um notebook poderá alcançar o patamar dos terahertz (isto é, mil gigahertz, ou um milhão de megahertz) superando a potência de todos os computadores existentes numa grande indústria. Poderemos utilizar computadores de mão tão potentes como os atuais domésticos e Workstations que gerenciarão milhares de computadores. Passaremos de memórias de gigabytes para memórias de terabytes. Assim, saltaremos de bilhões para trilhões de bytes. Já imaginou armazenar toda sua vida em um computador, todas suas experiências, momentos e sentimentos? Como parece, em breve isto será possível.

Fabio Cosman



A verdade sobre seu nº IP

Está se tornando cada dia mais comum o medo de invasões na internet. Pânicos causados por pseudo-hackers têm atormentado centenas de pessoas e muitas vezes simples ameaças destroem momentos de paz e diversão de uma forma irremediável. O mais impressionante é que estas ameaças, na maioria das vezes, são completamente sem fundamentos, não fazem sentido e algumas nem existem. Basta usar uma meia dúzia de siglas para dizer que vai invadir seu computador, e o que mais tem aterrorizado os internautas é: "Vou descobrir seu IP!"
Vão descobrir seu IP? Oh, que espanto, mas e daí? Segundo os terroristas, após descobrir o IP de uma pessoa, sua alma estará completamente enterrada na maldição eterna, pois poderão invadir, derrubar, espionar, remover, sacudir, esculhambar, destruir e remexer...

Um número IP é um endereço que todo internauta, assim que se conecta na grande rede, recebe. É através deste endereço que seus programas se comunicarão, seu navegador, seu ICQ, seu programa de e-mail etc. Este número não precisa ser fixo - e geralmente não é - e a cada conexão você recebe um número diferente.

IP significa "internet protocol", faz parte de um conjunto de instruções que permite a comunicação pela internet. Ele é responsável pelo encaminhamento correto dos pacotes de dados que trafegam na rede, de forma que eles sejam entregues corretamente ao seu destino.
Descobrir o IP de uma pessoa significa saber o "endereço internet"

Ip não tem nada a ver com e-mail
do seu computador naquele dia, ou durante aquela conexão. Somente isso, nada mais. O que se pode fazer com o IP de uma pessoa? Quase nada... se o computador não estiver com problemas do tipo "cavalos-de- tróia" ou semelhantes (ver capítulo 3), o número IP não vai servir para mais nada além de terrorismo.

Mesmo assim, dá para esconder o número IP?

Não, infelizmente não dá! Se por algum motivo seu computador não puder fornecer corretamente seu número IP, ele ficará incomunicável e sua conexão será desfeita. Ter um número IP faz parte da vida socialmente ativa dos computadores na internet e a comunicação depende disso. Alguns sistemas escondem esse número de outros internautas mas, pelo próprio bem da comunicação, eles são revelados. Por exemplo, bater papo requer que um computador se comunique com outro. Para isto ser feito, é necessário que ambos conheçam seus números IPs mutuamente pelo simples fato de precisarem saber com quem estão "falando".

É claro, sempre há as exceções: números IPs geralmente se mantêm os mesmos em redes físicas como escritórios e internet predial. Na maioria das vezes, estes números são fixos mas "mascarados" durante a comunicação externa por uma aplicação conhecida como "gateway" ou "proxy" e quase sempre, para quem está de fora desta rede, o número é genérico e inútil. Caso queira saber qual o seu número IP durante a conexão atual, um aplicativo distribuído com o próprio Windows dá as informações referentes. Vá em **Iniciar > Executar** e digite "**winipcfg**" (sem aspas).
Portanto, na próxima vez em que for ameaçado com seu próprio número IP, apenas dê uma gostosa gargalhada e volte para a sua tranqüilidade habitual. Já temos problemas demais para ficar nos preocupando com coisas que não existem!

A-há! Te peguei, hacker... mas, e agora?

É cada dia mais comum o surgimento de softwares que cuidam da segurança do seu computador pessoal e o mecanismo de monitoração mais utilizado é a "escuta" de portas de conexão.

Entretanto, de que adianta a informação de um hacker que tenta bisbilhotar nosso computador?

O que podemos fazer no momento em que descobrimos uma tentativa de ataque e conseguimos informações básicas sobre o hacker - como, por exemplo, seu número IP - através dos relatórios destes programas de proteção?
Primeiro, vamos analisar os fatos: um aviso emitido por um destes softwares de monitoração não significa que você está sendo invadido. É apenas uma notificação que houve uma tentativa de conexão em determinada porta. Muito provavelmente o hacker não obterá êxito pois os softwares de monitoração fazem uma checagem sobre as vulnerabilidades do computador, eliminando os programas ou falhas que permitiriam o ataque. Ficar de olho nas portas é uma medida secundária para quase todos estes programas de segurança.

Ao identificar uma tentativa de conexão, os programas registram dados importantes como hora, IP, tipo de ataque etc. e mostram estas informações a você, usuário. Estes dados são referentes ao computador de onde partiu o ataque e identificam de forma bastante confiável o responsável pela ação.
De posse destes dados, devemos, antes de qualquer outra ação, identificar a qual "provedor" pertence este número. Para isto, basta utilizarmos um comando do próprio Windows, dentro da janela do "Prompt do MS-DOS", executando: "**tracert 192.168.0.10**" (trocando o IP pelo número identificado no relatório).

Este comando produzirá uma série de linhas "percorrendo" o caminho de um pacote de dados do seu computador até o computador do invasor. Cada linha identifica um computador intermediário e as últimas identificam equipamentos do provedor de destino. Pelo nome destes equipamentos, é fácil deduzir a que provedor de acesso eles pertencem.
Através da página web do provedor, você pode conseguir um endereço de contato para reclamar sobre incidentes de segurança, abuse@provedor.com.br, mas uma maneira de garantir o recebimento da sua mensagem é enviar cópias para:
postmaster@provedor.com.br e root@provedor.com.br.

Com o endereço à mão, redija uma mensagem relatando a tentativa de acesso não autorizado ao seu computador pessoal partindo da rede sob a responsabilidade desta empresa provedora de acesso à internet. Repare que é esta empresa que responde pelas tentativas de invasão originadas na sua (dela) rede.
O fato do incidente ter sido provocado por um usuário é um problema do provedor com seu cliente em particular e, a você, cabe apenas a reclamação aos responsáveis pela rede. Não perca tempo tentando identificar o usuário.

Provedores sérios que se preocupam com sua imagem emitem uma notificação ao seu usuário (eles têm como identificar o usuário através do número IP e hora) avisando sobre as condutas aceitáveis dos seus clientes. Dependendo da política de cada provedor, o usuário, se estiver reincidindo nestas ações, pode ser bloqueado ou excluído.

A fim de botar a boca no mundo?

Crie seu weblog.

Lembra daquela menina, com seu diário, deitada na cama ou sentada em uma cadeira, escrevendo sobre o garoto da escola, relatando os últimos acontecimentos do dia ou tendo uma conversa com seu "eu" interior? Pois agora, ela está na frente do computador, colocando tudo na internet. Trata-se do weblogging, a nova mania dos internautas.

O weblog, também conhecido como blog, nada mais é do que uma página pessoal feita de pequenas e freqüentes notas.

O conteúdo pode variar bastante, dia a dia, comentários sobre sites, reflexões sobre política, destino da humanidade, álbum de fotografias, poesias, até palhaçadas em geral; dependendo da imaginação e dos propósitos do dono.

"O blog funciona como uma espécie de terapia. Você pode falar o que quiser, desabafar. É como fazer um diário mesmo. A única diferença é que seu irmão mala não vai precisar de nenhuma chave pra descobrir seus segredos. "É um bom passatempo", diz a estudante de jornalismo, Raphaela Rodrigues de 19 anos. Ela começou seu blog:
(http://inthejungle.blogspot.com),
há pouco mais de 1 ano, em um domingo em que eu estava em casa sem fazer nada.

"Resolvi então criar um blog justamente sobre isso... a arte de não fazer nada (o título do blog era "the art(e) of doin´ nothing").

Eu sempre conversava sobre isso com um amigo meu, ficávamos divagando sobre a importância de não se fazer nada.

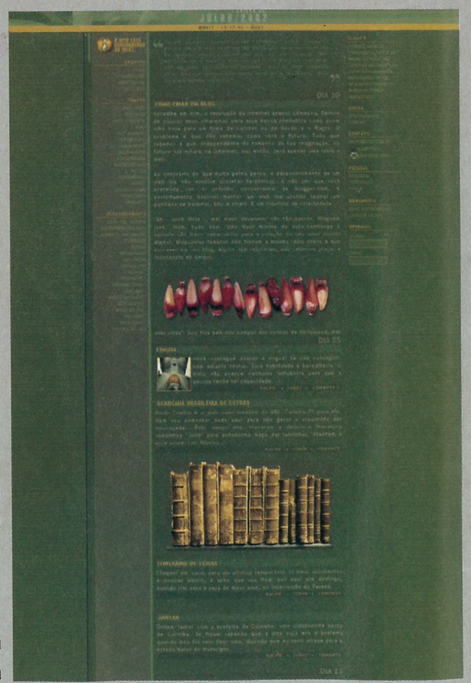
Mas minha vida ficou mais agitadinha (ainda bem),

Escrever sobre si mesmo ou sobre o cotidiano é uma das atividades mais antigas entre os internautas. Desde os primórdios da rede, usuários de todo o mundo se utilizam deste espaço para expressar suas idéias. Mas ter um blog virou febre a partir de 1999, quando um jovem americano chamado Evan William criou o BLOGGER: (www.blogger.com), site rápido e fácil de usar, direcionado aos escritores de plantão. Dois anos após seu lançamento, o site já conta com mais de 30.000 usuários. No Brasil, o site de blog mais famoso é o WebLogger Brasil (www.weblogger.com.br), que tem 11.000 usuários. Com eles, não é necessário - mas sempre ajuda - saber programar em HTML, Java, Flash e afins. Basta preencher um cadastro e utilizar os modelos de páginas prontas (templates) para sair escrevendo. Segundo Iglá Lear Generoso, da equipe da WebLogger, a faixa etária dos usuários varia de 16 a 25 anos.

http://www.boechat.com/tele/

A técnica em informática, 'Srta._Bandida', 23 anos, é outra usuária deste sistema. Internauta há cinco anos, ela conheceu o blog seis meses atrás, através de uma amiga que namorava um webdesigner. "Eu sabia que muita gente usava páginas pessoais para divulgar idéias, mas não conhecia esse sistema. Sempre gostei de escrever, com a facilidade desses sites, eu me senti motivada". O blog dela não é diário, ela preferiu usar esse espaço para publicar seus artigos sobre feminismo.

Mas por que dedicar tanto tempo do dia contando a outras pessoas fatos da sua vida ou falando sobre coisas que você acha interessante? Raphaela Rodrigues acha que escrever sobre coisas simples e corriqueiras é bom, engraçado, e além disso, "sacia essa vontade esquisita que o ser humano tem de querer invadir e/ou ter sua privacidade invadida".

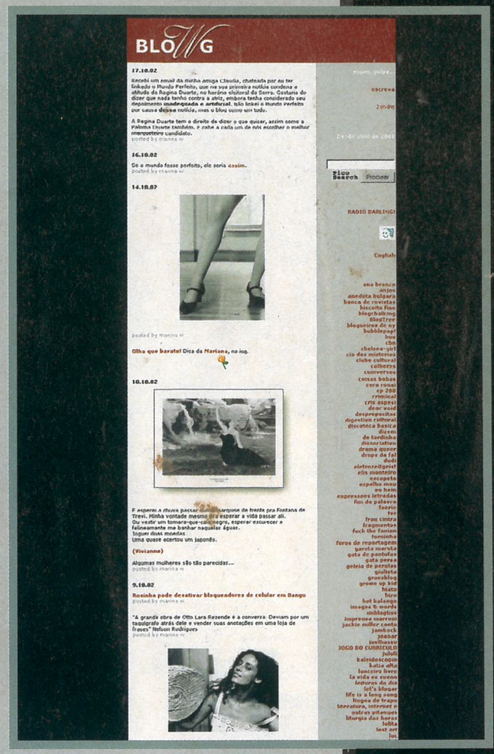

http://www.opio.com.br/

Dicas de como fazer um bom blog

O site "I´m on a roll": ('estou inspirado') (http://tirade.weblogs.com) traz algumas dicas legais para quem quer começar um blog, confira:

Se você for escrever um blog pessoal, escreva sem pensar, qualquer coisa que venha à cabeça, e depois deixe tudo lá, não se censure. Espere as pessoas se manifestarem sobre o que você escreveu.

Caso sua intenção seja escrever uma coisa mais informativa, é necessário conhecer e se interessar bastante pelo assunto. Não que você deva ser um expert, mas saber do que fala e poder fornecer material relevante para seus leitores. Recomendar sites, livros e material de apoio também é uma boa. Tudo para criar um diferencial e atrair um público grande e fazer seu blog ser visto.

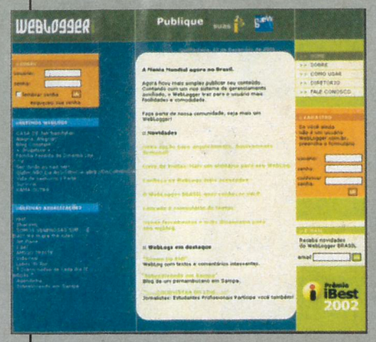


http://www.nathyfuknenemmm.blogspot.com
Bem, cheguei agora da rua, fui para quadra ver os meninos jogarem.
Foi muito bom, me diverti bastante
a noite estava deliciosa, bebi bastante
também! É legal, ficar assim rodeada de
gente bonita, eu gosto. Não gostava, mas
agora estou começando a descobrir um
mundo que sempre tive medo de tocar,
aquele mundinho que é feito de mistérios
e sensações... deu para sacar?

http://lilian.weblogger.com.br
Eu tinha uma galinha que se chamava
Marilú.
Um dia fiquei com fome e vendi a Marilú.
Peguei a grana, investi em ouro, lucrei
200% em menos de 1 mês.
Peguei o lucro, apliquei em ações, com 1
ano já estava bilionária.
Hoje em dia vivo numa província.
Não trabalho.
Freqüento a faculdade.
Não me relaciono com ninguém.
Vivo em anonimato.
E viva o Brasil!!!!!

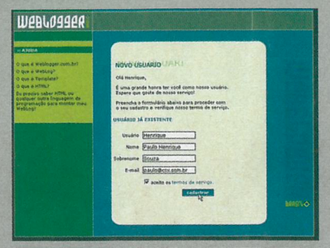
"how to blog" ("como blogar")

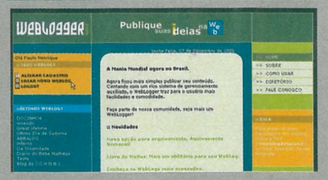
Criar o seu blog é muito fácil.
O processo é praticamente o mesmo em todos os sites, explicaremos aqui o do Weblogger, site nacional que hospeda blogs.



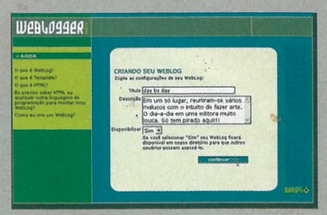
Entre em www.weblogger.com.br. No lado direito da página principal do site, onde está escrito 'Cadastro', digite seu nome de usuário, senha, confirmação

da senha e clique em OK.
Em seguida, digite seu nome, sobrenome, e e-mail. Clique em "cadastrar".
Após logar no sistema, no lado esquerdo superior, aparecerá o menu "Seus Weblogs". Clique em "Criar novo weblog".
Você poderá criar mais de um weblog na mesma conta, basta clicar em "Criar novo weblog" e repetir as instruções abaixo.

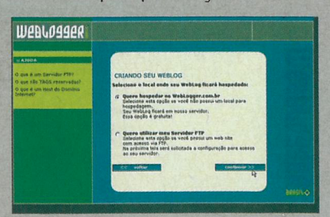




Se você selecionar "Sim", seu WebLog ficará disponível para que outros usuários possam acessá-lo.



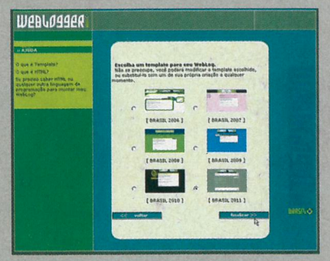
Em seguida, selecione Weblogger Brasil no local para publicação.



Dessa forma, seu weblog ficará hospedado no servidor deles. Lembrando que essa opção é grátis.

Na próxima tela, você terá que escolher um endereço (host) para seu WebLog.

Não utilize espaços em branco, apóstrofes, dois pontos ou caracteres especiais.
No formulário seguinte, escolha a aparência (template) do seu WebLog e clique em "finalizar".
Seu weblog está pronto.



Uma nova tela com o editor de texto aparecerá. Selecione o WebLog desejado e clique em "Editar Texto".

Digite seu texto na caixa central e clique em enviar na caixa de ferramentas (Atalho: Ctrl+Shift+S). Seu texto será publicado e aparecerá nesta caixa.
Logar novamente é tranqüilo. Entre no site da WebLogger e digite seu nome de usuário e sua senha no campo "Login". Selecione o weblog que você quer editar e mãos à obra.

incrementando
seu texto

*Para deixar seu texto em negrito, selecione o texto e clique em Negrito na caixa de ferramentas (Atalho: Ctrl+Shift+N).

*Para deixar seu texto em itálico, selecione o texto e clique em Itálico na caixa de ferramentas (Atalho: Ctrl+Shift+I).

*Para inserir uma imagem, clique em Imagem na caixa de ferramentas, selecione e digite o local de origem (que pode ser qualquer servidor). Em seguida clique em inserir imagem.

*Para colocar um contador, clique em "Template", coloque a TAG <#weblogContador#> no local desejado e clique em: "salvar alterações".

*Para inserir um link, clique em Link na caixa de ferramentas e digite a url desejada.

*Para publicar o texto em seu WebLog, clique em enviar.
*Para visualizar textos anteriores publicados em seu WebLog, clique no dia desejado no calendário.
Inspiração

Você já viu o que é blog, já sabe como montar um e sabe até como torná-lo atraente, mas não tem a menor idéia do que vai escrever, aqui vão dicas de alguns sites para ajudá-lo.

*http://www.eatonweb.com
Este é o primeiro site de blog de que se tem notícia. Sempre atualizado, começou como um bookmark e hoje já possui mais de 500 colaboradores.

*http://tv.blig.ig.com.br
Quer ver o que rolou na Casa dos Artistas mas não foi mostrado na TV? Entre e confira.

*http://semlove.weblogger.com.br/
Se o blog é para ser um diário, esse aqui é o estereótipo, feito por um grupo de amigas sem namorado. Ele traz comentários sobre o dia-a-dia e desilusões amorosas.

*http://subterrane.com/
Um blog bem simples e de navegação ágil.

*http://home.twcny.rr.com/edgerton/er/blog/index.html
Gosta ou gostava de Plantão Médico (a série de TV)? Mantenha-se informado neste blog.

*www.nathyfuknenemmm.blogspot.com
O que acontece quando uma garota está com raiva do mundo?

Agora, que você já sabe como é um blog, é só botar a boca no mundo!

VIDA E MORTE DE UM HACKER

"Leia com atenção o texto abaixo, pois é a história do que eu fiz, de como amei a vida e porque desisti dela.

Eu era um adolescente normal como qualquer outro, mas tinha uma visão de vida pela qual muitos teriam me invejado. Não tinha muitos amigos mas era feliz. Recebi uma criação invejável, podia sair e voltar de casa a hora que quisesse, e recebia dos meus pais toda atenção que necessitasse. Apesar disso não saia de casa com a freqüência de um adolescente normal, não pelo fato de ser anti-social, muito pelo contrário fazia amizade muito fácil, também não era um "nerd" era o típico aluno desatento, sobre o qual os professores se reuniam para queixar-se, gostava de entrar em brigas e odiava ir para a escola aprender as mesmas coisas todo dia. Odiava a história com tanta injustiça, escravidão de negros, preconceito contra índios, judeus ou estrangeiros. Não tinha uma vida muito agitada, cheia de viagens, mas acreditava ter nascido no ano certo, pois estava acompanhando todo o desenvolvimento da tecnologia.

Meu único medo era saber que tudo isso, uma hora pudesse acabar. Um dia me deparei com uma máquina incrível que quase não tinha limites, se bem utilizada... um computador. Eu estudei muito (engenharia da computação e ciência da computação) mas tornei-me um hacker. O que eu tinha em mente? Mudar o mundo; durante dois anos dediquei-me a invadir e roubar informações dos militares americanos. Eu tencionava roubá-las, entendê-las e depois divulgá-las. Quase consegui alcançar o meu objetivo; meu erro foi que depois de invadir sistemas militares, nos quais não podia ficar mais de um minuto, eu fiquei autoconfiante demais. Um dia estava em casa montando uma pequena home page que iria mostrar ao público todas as informações que roubara, quando fui abordado por agentes federais que me pegaram às 3:40h de algum dia do ano de 1996.Você não vai encontrar nos jornais sobre mim, ou, quando muito, apenas algumas linhas que dizem: "polícia pega vândalo destruindo telefones públicos e descobre em sua casa centenas de cartões de crédito falsos". Eu nunca falsifiquei nenhum cartão de credito, meu único ato criminoso foi invadir sistemas do governo e copiar informações confidenciais. Fui condenado a sete anos de prisão sem direito à condicional , e fui proibido de usar computadores até o fim da vida.

"TENHO CÓPIAS ESCONDIDAS DE TUDO QUE DESCOBRI, E ESPERO..."

Outro dia eu li nos jornais sobre dois garotos que mataram um mendigo queimado enquanto dormia, e que um deles era filho de um juiz criminal. Hoje pego o jornal e leio: "Garotos confessam o crime mais não vão a julgamento". Chega! Eu cansei de viver em um mundo onde assassinos ficam na rua enquanto aqueles que estão em busca de uma vida melhor ficam na cadeia, cansei de ter que aceitar o fato de que estou privado daquilo que eu amo e faço melhor, ser um hacker... cansei de saber que os nossos governantes querem um povo ignorante, o qual eles possam manipular e enganar, dizendo que estamos na terra da liberdade.

Um país que tem uma tecnologia dez anos à frente da atual e que se fosse colocada a serviço da humanidade, poderia melhorar sua vida em cem por cento. Estou cansado de viver em um mundo em que o governo nega recursos para a educação ao mesmo tempo que os aplica em equipamentos militares para garantir sua superioridade perante ou outros países. Agora eu pergunto: Como, com tudo isso, eles ainda podem falar em globalização? Hoje eu tenho vergonha de ser americano. Agora só me resta a esperança de que um dia os hackers do mundo se unam e mostrem à humanidade a verdade.

Tenho cópias escondidas de tudo que descobri, e espero que a pessoa que colocar meu manifesto na rede, também coloque todas as informações pelas quais eu fui preso".

O hacker foi encontrado em sua cela com os pulsos cortados, foi levado ao hospital do presídio onde morreu às 4:32 do dia primeiro de janeiro de 1998.

O seu amigo, que ficou encarregado de colocar seu manifesto e as outras informações na rede, foi até o local indicado, onde estariam as cópias dos arquivos confidenciais, mas foi pego pela polícia federal e respondeu a processo e foi obrigado a pagar uma multa no valor de US$ 80.000.

O texto acima é de autor desconhecido.

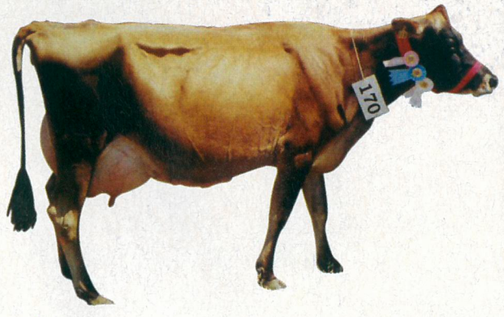
Soul Hacker by Felipe Lucca

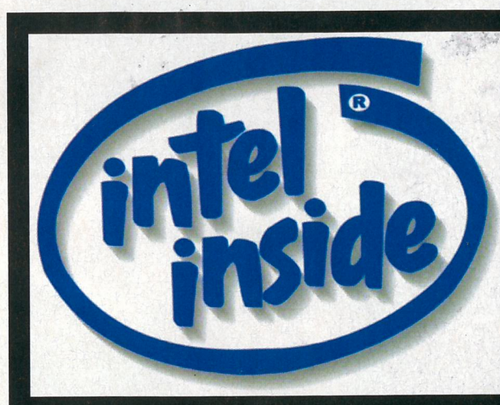
Maior encontro de hackers da história

Hackers de todo o mundo participaram nos dias 6, 7 e 8 de agosto de uma espécie de campeonato mundial de invasores de sistemas, em um acampamento ao ar livre em Paulshof, próximo a Berlim. O evento foi organizado pelo grupo alemão Chaos Computer Club (CCC) e o objetivo era transformar na maior concentração de hackers da história da informática. A página Web www.ccc.de/camp, traz todas as informações sobre o encontro. Uma das tarefas no "hackcenter" foi invadir em tempo real áreas mantidas por outras equipes. Detectar a invasão e "derrubar" os adversários também contam pontos na competição.

O governo de Gujarat na Índia ordena salvação das vacas

Na Índia, o ministro da Proteção de Vacas do partido nacionalista hindu, Haren Pandya, declarou que: "Se decidiu que os líderes de estado devem incentivar a salvação da vida das vacas, para que outros possam seguir o exemplo."Este é o único estado da Índia que tem um ministério exclusivamente dedicado a proteger as vacas, que como se sabe são considerados animais sagrados pelos hindus. O problema é que essa região sofre com uma seca como não se via nos últimos 100 anos. Mas como disse o ministro, é responsabilidade dos cidadãos salvar os bovinos. Será que a vaca louca também é cultuada por lá?



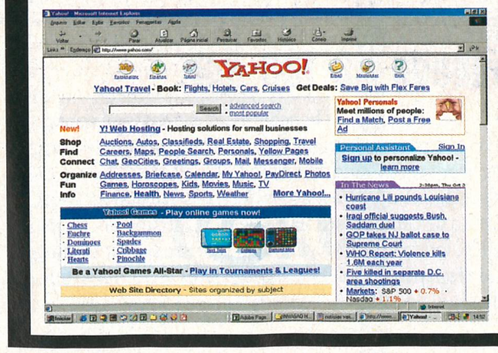


Intel é processada e pode parar produção de Pentium 4

A Intel foi processada pela Via Technologies e, caso condenada, poderá ter de parar a produção de Pentium 4. O processo foi movido pela Centaur, uma subsidiária da Via Technologies. A Intel e a Via Technologies são rivais no mercado de processadores mas ocasionalmente também sócias. O centro da nova disputa na justiça é uma patente que a Centaur detém do modo de organizar data no Pentium 4. As duas empresas já estiveram envolvidas em disputa judicial em 1999. O motivo também era relacionado a patentes, no caso do Pentium III. A Intel venceu a disputa e também seria a detentora da patente do Pentium 4, idéia contestada pela Via Technologies este ano.

Hacker altera notícia publicada pelo Yahoo

O hacker Adrian Lamo revelou como alterar notícias no Yahoo sem permissão, acessando o sistema de administração de conteúdo usado pelo site. Na demonstração, Lamo acrescentou citações falsas para demonstrar a possibilidade ao noticiário Security Focus. O Yahoo já anunciou que a falha foi detectada e corrigida. O ocorrido, contudo, levantou a questão do perigo de alterar informações em importantes sites com notícias. O portal Yahoo é um dos mais populares da Internet, apresentando em junho passado mais de 200 milhões de visitantes. Lamo usou servidores proxy que conectam a rede interna do Yahoo à Internet para realizar a invasão. Ele configurou seu navegador para driblar o proxy e ganhar acesso às aplicações disponíveis na rede interna do portal. A partir dali, Lamo não encontrou barreira de senhas que impedissem a alteração do conteúdo publicado. O hacker acrescentou em sua demonstração uma citação falsa, em uma matéria sobre o programador russo Dmitry Sklyarov acusado de desenvolver um programa que permite copiar livros eletrônicos sem permissão. A citação dizia ironicamente que o trabalho de Sklyarov levantou "o fantasma do acesso irrestrito das minorias excluídas à literatura". Além disso, atribuiu ao presidente dos EUA George W. Bush a citação de que "algumas crianças poderiam ter acesso aos trabalhos de Mark Twain e Foucault, mas que essa ilegalidade flagrante não poderia continuar. Qualquer um que disse a elas que a verdade as libertará, certamente não está familiarizado com as leis federais". Fonte: PCWORLD



Hacking pode se tornar Ato de Terrorismo nos EUA

Hackers e advogados de privacidade ficaram desnorteados quando souberam que o governo dos Estados Unidos planeja fazer uma mudança na legislação, passando a considerar o cyberterrorismo como ato de terrorismo. O resultado seria a prisão perpétua sem direito a fiança, como acontece hoje em dia aos atos terroristas. No encontro que aconteceu no Capital Hill esta semana, o Departamento de Defesa Americano teria pedido a Bush que desse continuidade ao Ato Antiterrorismo no Congresso. A proposta de 25 páginas, da ao Governo plenos poderes para vigilância eletrônica, como acesso as conversas telefônicas, além de outras técnicas que serão usadas futuramente para detectar supostos terroristas. O documento contém uma lista de "Ofensas Terroristas Federais" que inclui entre eles, assasinato de fedderais, atentado a bomba, homicídios, entre outros. Inclui também fraude por computador, tornando efetivo o ato terrorismo de invadir computadores com o propósito de vandalismo, roubo de informações valiosas ou lançar um programa que intencionalmente compromete o sistema, como um vírus.

Estupro com uma boneca inflável

A polícia de Palma de Mallorca na Espanha recebeu uma chamada de um grupo de jovens que queriam denunciar uma agressão sexual a uma menor. Os agentes chegaram rapidamente ao local indicado e encontraram dentro de um carro um homem efetivamente com uma menor inflável. Os jovens não haviam reparado que, na realidade, a companheira do amante motorizado era uma boneca inflável.

Falha grave põe em risco redes privadas da Microsoft

Uma falha em um aplicativo da Microsoft pode expor as intranets corporativas a sérios riscos de segurança, alertam especialistas. O problema, divulgado pela empresa austríaca phion Information Technologies, afeta serviços baseados no protocolo PPTP (Point-to-Point Tunnelling Protocol), fornecidos com o Windows 2000 e XP e usados em redes privadas virtuais (VPN) da Microsoft As VPNs normalmente são utilizadass em empresas para que os funcionários possam conectar-se remotamente a suas redes internas, usando canais criptografados em uma rede pública. Como são consideradas seguras, as VPNs oferecem elevados privilégios de acesso, o que aumenta o perigo caso o sistema apresente falha. O especialista Marc Maiffret, da eEye Digital Security, foi um dos que chamou a atenção para a gravidade do problema. "Se alguém penetrar no seu servidor Web, isto é mau, mas não é o fim do mundo. Mas se alguém entrar na sua VPN? Há muito pouca segurança dentro de um rede local", disse o especialista, segundo o site de tecnologia Silicon.com. A Microsoft já foi avisada do bug e garante que está tomando providências para tapar o furo o mais breve possível. A phion informa que ainda não há uma solução definitiva para o problema, mas sugere como paliativo para o Windows XP que se filtre a porta dos serviços PPTP através do firewall nativo do sistema. Para o Windows 2000 não se conhece contorno semelhante. A empresa afirma que não irá fornecer programas (exploits) para demonstrar o bug, certamente devido a sua gravidade. Maiores detalhes podem ser encontrados em http://www.phion.com/adv/index.html

Kevin Mitnick está autorizado a trabalhar

O hacker mais famoso do mundo terá como acessório para o trabalho apenas uma máquina de escrever. Após ter sido afastado de computadores, celulares e de qualquer outro equipamento que permita o acesso online, Kevin Mitnick muda radicalmente sua forma de pensar e convence as autoridades de que o trabalho enobrece o homem.Kevin Mitnick foi convidado a escrever uma coluna para a revista americana Contenville, especializada em segurança na internet, mas o uso de uma simples máquina de escrever foi a condição sine qua non para que o FBI permitisse o início de uma nova carreira para o hacker. Mitnick passou 5 anos na prisão, respondendo processos sob as acusações de pirataria e invasão aos sistemas de grandes empresas, como Motorola, Novell, Nokia e Sun Microsystems.

Hacker brasileiro pode ter roubado R$ 100 mil

Guilherme de Oliveira, 18 anos, está sendo acusado de invadir o sistema de vários bancos, além de retirar de contas bancárias pelo menos R$ 100 mil, provocando prejuízo para empresas e pessoas físicas. O hacker foi preso em setembro de 2002, em Campo Grande, e foi libertado alguns dias depois, de acordo com informações do Campo Grande News. O computador do rapaz está sendo periciado. O delegado titular da delegacia de defraudações, Reinaldo Amaral garantiu que o computador foi manipulado apenas pelos peritos do Instituto de Criminalística. O delegado aguarda um laudo sobre o conteúdo do computador. Ainda de acordo com o delegado, foram identificadas várias pessoas supostamente envolvidas no caso. Outro inquérito foi instaurado para apurar as responsabilidades destes supostos envolvidos, que estariam em São Paulo, Rio de Janeiro, Campo Grande e Corumbá

VÍRUS ESPIÃO ENVIA MENSAGENS EM MASSA

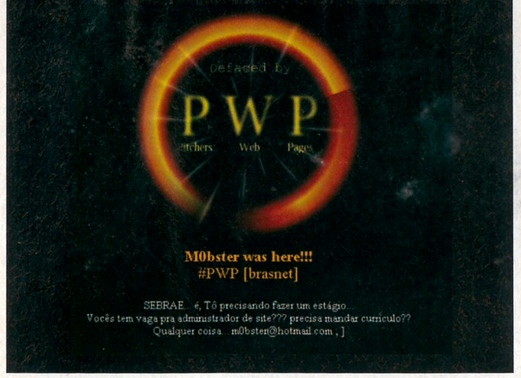
O vírus W32.Bugbear@mm envia e-mails em massa, se espalha por drives de rede e também age como espião. De rápida disseminação, tem classificação de risco acima da média. O Bugbear chega numa mensagem de e-mail com assunto variável e um anexo com extensão EXE, SCR, ou PIF. Se o usuário abrir o anexo, o invasor se autocopia para a pasta Iniciar do Windows, a fim de garantir sua execução durante a inicialização da máquina. Em seguida, o Bugbear cria três arquivos DLL no diretório de sistema (iccyoa.dll, Igguqaa.dll e roomuaa.dll) e dois DAT (okkqsa.dat e ussiwa.dat) na pasta do Windows. O invasor usa máquina SMTP própria para enviar e-mails a endereços que coleta na máquina invadida. Além disso, ele se dissemina para drives de rede. Para tentar agir mais à vontade, o Bugbear tenta desativar os processos dos principais programas antivírus e firewalls disponíveis no mercado. Passa de 100 a lista dos arquivos que ele está preparado para neutralizar. O Bugbear também funciona como programa-espião. Assim, ele permite acesso externo à máquina contaminada. Vale ainda destacar outro aspecto importante: o Bugbear explora uma vulnerabilidade do Internet Explorer 5.x para executar o anexo automaticamente, sem qualquer intervenção do usuário. Para baixar a correção para essa falha do IE 5.x, vá ao endereço www.infoexame.com.br/aberto/download/2315.shl.

Site do PT é hackeado

O site oficial do Partido dos Trabalhadores (PT) permaneceu fora do ar em pelo menos duas ocasiões nas vésperas das eleições, mas não foi por excesso de visitas, depois da vitoriosa campanha de Lula no primeiro turno das eleições para presidente. O site foi tirado do ar pelos próprios administradores do sistema, para corrigir falsas notícias colocadas por um cracker na página principal. Usando o apelido de WhiteHat, o invasor trocou as manchetes por outras como: "Mais segurança na Internet", "The WhiteHat na área" e "Abraço pro Moondog" (provavelmente algum amigo seu, integrante do submundo da rede). Também publicou o seu endereço de e-mail na página, na forma "nosdeumachance arroba hacker ponto am". O site passou apenas alguns minutos alterado, e neste momento pode ser acessado normalmente, mas InfoGuerra conseguiu com exclusividade duas cópias das páginas desfiguradas, além de fazer contato com o cracker. Ele admite que o ataque se deve ao fato de que o site do PT teria muita visitação hoje e todos estariam de olho nas notícias, mas ao mesmo tempo afirma que não teria tido êxito se não fosse uma falha de programação do sistema. "A falha já existia há muito tempo, mas eu esperei o momento certo para fazer o ataque", disse. Ele afirma que todos os sites de candidatos à presidência apresentam o mesmo bug chamado de SQL Injection e que dá acesso não-autorizado ao servidor por meio de caracteres reservados, como apóstrofo ('). WhiteHat também garantiu que "a vez do Serra vai chegar", mesmo com o site deste presidenciável utilizando um banco de dados diferente. O cracker afirma ainda que conseguiu acessar dados de militantes do PT, como nome, e-mail e título de eleitor, mas não se interessou porque não viu "nada de útil nisso". WhiteHat também mandou um recado para Lula, relacionado a segurança na Internet: "Como o Lula já está quase lá, o intuito real é que ele saiba disso e atente também para o lado online da coisa, pois no governo, ele sempre será alvo de ataques." Foram enviadas mensagens para vários endereços de e-mail presentes na seção "Fale conosco" do site, mas até o momento de publicação desta notícia a única resposta recebida veio do endereço: presidencia@pt.org.br e trazia o texto, "Obrigado pela sua mensagem. Esta é uma resposta automática. Assim que for possível lhe responderemos. Atenciosamente, Assessoria da Presidência Nacional do PT".

Hacker pede emprego no site do Sebrae

Um grupo hacker invadiu a página do Sebrae na Paraíba. A mensagem assinada por Mobster era também um pedido de emprego. Estava escrito: "SEBRAE... é, Tô precisando fazer um estágio... Vocês têm vaga pra administrador de site? precisa mandar currículo?". Sem abraços ou saudações para amigos e outros grupos hackers, como se costuma ver em invasões deste tipo. Segundo o Alldas, as primeiras invasões do grupo foram registradas no mês de julho.



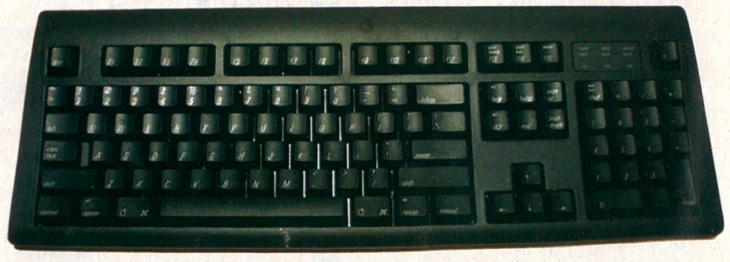
Mulher tida como morta ressuscita em funerária dos EUA

O diretor de uma funerária na cidade de Ashland, nos Estados Unidos, tomou um grande susto quando uma mulher, dada como morta pelos médicos, começou a se mexer na funerária. A mulher fora encontrada inconsciente em uma banheira cheia de água fria, depois de ter tomado uma dose excessiva de comprimidos, de acordo com a polícia. Os médicos de emergência que a atenderam não conseguiram encontrar sinais de vida e a mulher, depois que os policiais "atestaram" morte por suposto suicídio, foi levada para a funerária. O Departamento de Saúde Pública abriu sindicância para determinar se a equipe médica de emergência agiu corretamente. "- Não terem levado a mulher para um hospital foi um grave erro. Pessoas com baixa temperatura e cor azulada podem ser ressuscitadas", disse Murray Hamlet, especialista em casos de severa hipotermia.

O que tem dentro do seu teclado?

Quem é que nunca passou horas na frente do computador comendo um biscoito ou tomando café? Invariavelmente, o teclado sempre acaba recebendo migalhas e outras sujeirinhas mais. A sociedade Reading Scientific Services analisou as porcarias encontradas dentro dos teclados. Os resultados são:

Cereais: 15%
Biscoitos doces e similares: 15%
Clips: 7%
Vegetais diversos: 4%
Folhas: 1%
Pontas de lápis: 1%
Unhas: 1%
Insetos: 1%
Papel Alumínio: 1%
Pelos: 1%



Mais informações podem ser encontradas no site oficial da Reading Scientific Services: www.rssl.co.uk.

Máquina que produz orgasmos

O doutor Stuart Meloy, anestesista e especialista em tratamento de dores em Winston-Salem, N. C., assegura ter criado uma máquina que produz orgasmos. Sua descoberta foi acidental. Quando estava tratando de uma mulher com dores nas costas, Meloy não posicionou corretamente o eletrodo, o que é bastante habitual e normalmente causa dor. Segundo o médico, o som que a paciente emitiu foi "um pouco diferente", e por isso ele perguntou a ela quais teriam sido suas sensações. Ela lhe contou que havia tido um orgasmos e de quebra perguntou se ao médico se ele poderia ensinar o truque ao seu marido

Hackers atacam FHC novamente

Já deixou de ser novidade... O grupo de hackers que assina "Resistência 500" voltou a atacar . Invadiram servidores do governo federal, redirecionando o site do Ministério da Ciência e Tecnologia para uma página com críticas ao governo de Fernando Henrique Cardoso.

Preso o hacker que invadiu o site das forças armadas americanas

O FBI prendeu, na última segunda, Chad Davis, um jovem de 19 anos, sob a acusação de ter crackeado o site das Forças Armadas dos Estados Unidos em junho deste ano. Os agentes federais chegaram até Davis através de seu nickname: Mindphasr. Ao que tudo indica, Davis, que mora sozinho num apartamento em Green Bay, Wisconsin, é o fundador do grupo de hackers Global Hell (gH), que clamou responsabilidade pelos ataques digitais realizados a vários sites americanos nos últimos meses (como o da Casa Branca, do Departamento de Agricultura e do próprio FBI).

Adote uma ovelha via web e receba benefícios

A região dos Abruzzos, no centro da Itália, está perdendo parte de sua identidade. Há algusn anos imensos rebanhos de ovelhas foram sumindo gradativamente dos pastos da região. Devido a emigração, o modo de vida de seus habitantes e as enfermidades, a população ovina quase que desapareceu. Agora a empresa italiana Manuela Cozzi organizou uma louvável campanha em defesa da ovelha local, e a lançou por meio da Internet. Você e qualquer pessoa (ou empresa) de qualquer parte do mundo que queira adotar uma ovelha, pode fazê-lo pelo módico preço de 350.000 liras (uns 150 dólares). A empresa compensará o esforço dos benfeitores a cada ano com cinco quilos de queijo, três de requeijão e com a lã do animal como preferira: tal qual, lavada ou em forma de calças.

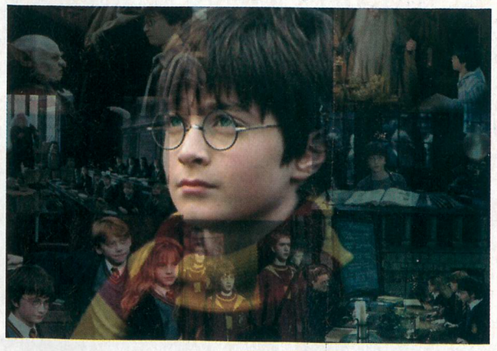
Se interessou, entre em: http://www.asca.dimmidove.com/

Hackers invadem a Holanda

Geeks estão chegando à Holanda vindos de todas as partes do mundo para a convenção Hackers at Large. Devido aos recentes acontecimentos, o evento tem mais importância do que nunca. Por Steve Kettmann. As centenas de hackers que chegaram à Holanda essa semana para os três dias de conversas e workshops estavam furiosos. Eles estão descontentes com o fato de o movimento hacker estar sendo demonizado e desprestigiado por pessoas que sabem muito pouco do que estavam falando.

Harry Potter e Satanás

Os livros de Harry Potter escritor por J. K. Rowling são voltados para as crianças, mas algumas pessoas têm encontrado uma relação entre essas histórias infantis e "Satanás". Por exemplo, na Internet o grupo cristão Freedom Village USA disseram que "os livros de Harry Potter são armas de recrutamento para a bruxaria e o oculto". Para eles, um claro exemplo do culto ao "demônio" é o episódio de 6 páginas que começa na página 66, com o que teríamos o número 666, o sinal do anticristo. Nos Estados Unidos existe um legado querendo criar uma associação, "Muggles For Portter", com a mesma opinião. E a briga vai começar com a Associação dos Editores Americanos e a Coalizão Nacional Contra a Censura. E perguntamos: será que essa gente não tem nada melhor pra fazer do que encher o saco com esse papo de capeta?



Companhia de seguros distribui vídeos pornográficos

A companhia de seguros holandesa National Nederlanden, estava em plena campanha de promoção de seus produtos especiais para pensionistas. Entre outros meios, a empresa utilizou alguns vídeos que seus vendedores distribuíram a possíveis clientes. Em um dos lotes de 500 fitas, o distribuidor incluiu erroneamente... 100 fitas pornográficas. Segundo o porta-voz da companhia, este assunto é "muito doloroso" para eles.

Bom, de qualquer forma, os velhinhos devem ter ficado agradecidos...

Pedreiro morde cachorro e quase é linchado

O pedreiro Jair Rodrigues da Silva, 32 anos, morador do Bairro Profilurb, em Americana,a 140 quilômetros de São Paulo, atacou um cão mordendo o focinho do animal e batendo com um pau. Silva ficou muito nervoso ao ser mordido pelo um cão. A cena chamou a atenção de pessoas que passavam pela Rua Antonio Conselheiro , que chegaram a agredir o pedreiro. A Guarda Municipal foi chamada e evitou um começo de linchamento. O pedreiro e o cachorro foram encaminhados ao Plantão Policial onde foi lavrado um boletim de ocorrência. "Tiramos umas dez pessoas de cima do moço", conta o soldado Augusto, da Guarda de Americana, que encaminhou "as vítimas" ao atendimento. Silva passou pelo Pronto-Socorro e o cachorro foi levado ao Centro de Zoonose de Americana onde permanece em observação. Conforme o boletim de ocorrência lavrado pelo 4º DP, Silva cometeu crueldade contra animais de acordo com a lei 9099 que dispõe sobre crimes de menor poder ofensivo. Se condenado, pode pegar até 1 ano de detenção.

Netscape pode estar espionando buscas na Internet

De acordo com um teste realizado pela Newsbytes, o browser Netscape, de propriedade da AOL Time Warner, estaria capturando todas as palavras utilizadas na barra de buscas do Navigator e as enviando para a url info.netscape.com junto com o endereço IP do usuário e um número único de identificação. Dessa forma, a Netscape poderia estar compilando uma base de dados das principais buscas realizadas pelos usuários, além de poder identificá-los toda a vez que realizassem uma nova busca.

O garoto que dispara alarmes

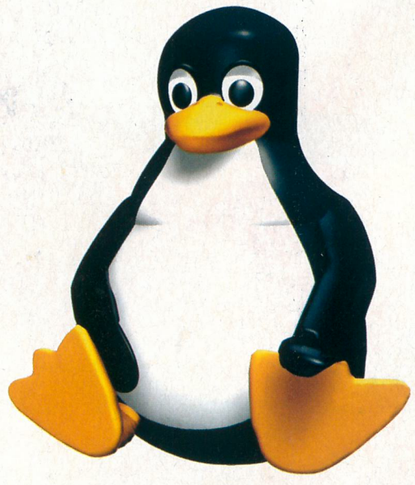
Se você não sabe como se vingar de alguém, saiba que tem gente que facilita seu trabalho. No site ww.doggypoop.com, você pode encomendar três modelos diferentes de fezes de cachorro para mandar a quem quiser. Pelo preço módico de 14,95 dólares, você leva 500 gramas e com 19,95 pode logo adquirir 1 quilo de "caquinha" de cachorro de boa qualidade. Através disso, podemos perceber o avanço do comércio em certos aspectos inesperados.

Shakespeare fumava maconha

Frances Thackeray e Nick Van de Merwe, cientistas sul-africanos, asseguram que Shakespeare fumava maconha. Eles estudaram os restos que havia na residência do escritor em Stratford-upon-Avon, e encontraram a erva em várias tigelas de argila. Agora se explicam algumas das visões de Hamlet e as alucinações e seres fantásticos que aparecem em algumas de suas obras. Também asseguram que isso pode explicar a grande produtividade do escritor. Desde o século XVII se conhecia a planta da maconha na Inglaterra, e não somente em seu uso tradicional, como também nos " lúdicos" .

Bug no Linux permite invasão do sistema

Uma falha encontrada na amplamente utilizada biblioteca de compressão zlib pode permitir que usuários mal intencionados ataquem serviços variados em sistemas Unix, podendo até mesmo executar código arbitrário remoto.



SPOOFING

ENGANANDO , DERRUBANDO E INVADINDO

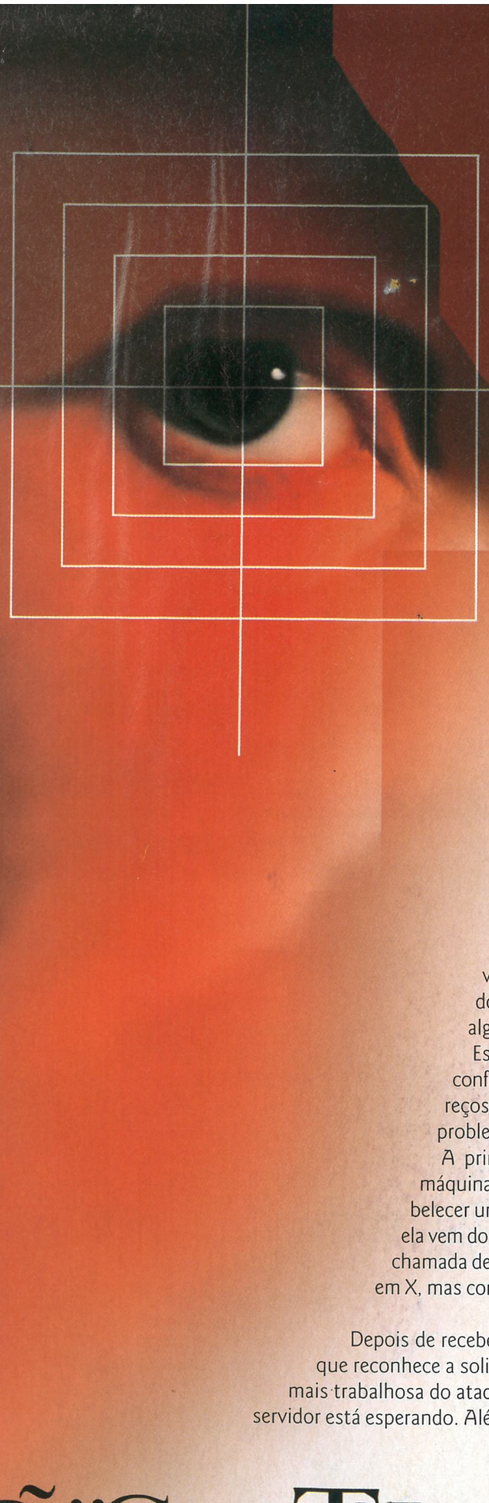
Certamente a frase que mais ouvimos de nossos pais quando somos criança - depois de "não faça isso" ou "não faça aquilo" é claro - é: "não converse com estranhos".
Isso porque pessoas desconhecidas podem ter más intenções, ou querer se aproveitar de nós.

Num mundo de insegurança e guerras como o de hoje, confiar em quem conhecemos já é uma grande aventura, em quem nunca vimos então, é pedir demais.

Em networking (internet, ethernet etc.), isso também acontece. Várias comunicações entre computadores se baseiam nesse princípio de "trusted hosts", ou seja, "parceiros confiáveis". Os computadores se comunicam sem a necessidade de uma constante verificação de autenticidade entre eles. Em certos sistemas, com a intenção de obter um melhor nível de segurança, o servidor de rede só libera a utilização de certos serviços a um número restrito e autenticado de usuários, que não são "estranhos" para ele.

O método encontrado para furar este esquema é o de falsificar o remetente dos pacotes de dados que viajam na rede. Essa técnica é conhecida por spoofing.

Disfarce, é basicamente isto o que o spoof



faz. O ataque acontece quando o invasor fabrica um pacote contendo um falso endereço de origem, fazendo com que o host atacado acredite que a conexão está vindo de um outro local, geralmente se passando por um host que tem permissão para se conectar a outra máquina. Fica mais fácil com esse esquema:

Acesso Confiável
Servidor 1 ——— Servidor 2

O invasor irá dizer ao Servidor 2 que seu DNS/IP é o do Servidor 1, tornando possível a conexão. "Por que eu não ouvi meus pais?"

Vulnerabilidade

O spoof é um ataque ao qual não estão sujeitos todos os sistemas operacionais. Somente aqueles rodando uma versão completa do TCP/IP, como os Unix likes. Ou seja, máquinas rodando Windows ou DOS não são vulneráveis. Mas Mac rodando A/UX e PCs rodando Linux podem estar vulneráveis sob certas circunstâncias: se estiverem utilizando o X-Windows System, Serviços Remotos (R Services), ou algum tipo de NFS mal configurado.

Esse método de ataque funciona porque os serviços de confiança das redes se baseiam apenas na autenticação de endereços. Como o IP pode ser facilmente mascarado, não há muito problema em aplicar essa técnica.

A primeira etapa de um ataque por spoof é identificar duas máquinas de destino. Uma vez identificadas, o invasor tentará estabelecer uma conexão com o Servidor 2 de forma que ele acredite que ela vem do Servidor 1, quando na verdade vem de sua própria máquina, chamada de X. Isso é feito através da criação de um pacote falso (criado em X, mas com endereço de A) solicitando uma conexão com o 2.

Depois de receber esse pacote, 2 responderá com um pacote semelhante, que reconhece a solicitação e estabelece números de seqüência. Essa é a parte mais trabalhosa do ataque, pois é preciso adivinhar o número de seqüência que o servidor está esperando. Além disso, é preciso impedir que o pacote de 2 chegue até 1.

Se isso acontecesse, 1 negaria a conexão e o ataque falharia. Para isso, o invasor envia diversos pacotes a primeira para esgotar sua capacidade e impedir que ele responda a segunda vez.

Uma vez que essa operação tenha chegado ao fim, a falsa conexão poderá acontecer.

Hackers – Resposta e Contra-Ataque

Empresas de todo o mundo já foram vítimas de centenas de ataques por computador, que originaram extorsões, furtos de propriedade intelectual e diversos outros crimes de rede. Atualmente, a maior parte desses incidentes de segurança ou de crimes por computador tem base em comportamentos que já são proibidos por lei, como furto de informações, espionagem e acesso não autorizado. Para tanto é necessário ter um mecanismo de reação que avalie a situação com precisão, promova uma rápida recuperação dos dados e coíba os ataques, investigando os incidentes e tomando medidas legais ou administrativas contra os agressores que danifiquem o seu patrimônio. Os chamados "crimes de computador" acarretam problemas para as empresas e criam o desafio de: Impedir o furto de informações proprietárias e confidenciais proteger a privacidade e o bem-estar dos empregados e dos clientes. Este livro demonstra, ao longo de seus capítulos, diversas técnicas que ajudam a coletar provas que confirmem a existência de atividades de computador ilegais, não autorizadas ou inaceitáveis, e também oferece técnicas para determinar a identidade dos responsáveis por tais atividades.

Autor: Chris Prosise - R$ 69.00

A preparação do Spoofing

O spoofing só funciona se todas as máquinas participantes utilizem o FULL TCP/IP, esse ataque exige que os servidores rsh e rlogin e rexce estejam em execusão no momento em que o IPSpoofing for realizado.

O UNIX e suas variantes, como o Linux oferecem estes serviços nativos no sistema operacional. Já o Windows não conta com nenhum destes serviços. Sendo assim você deve utilizar o Linux em suas redes locais enquanto estiver experimentando o IPSpoofing.

Pode-se verificar se esses serviços estão disponíveis através de uma varredura de portas na máquina-alvo com os serviços:

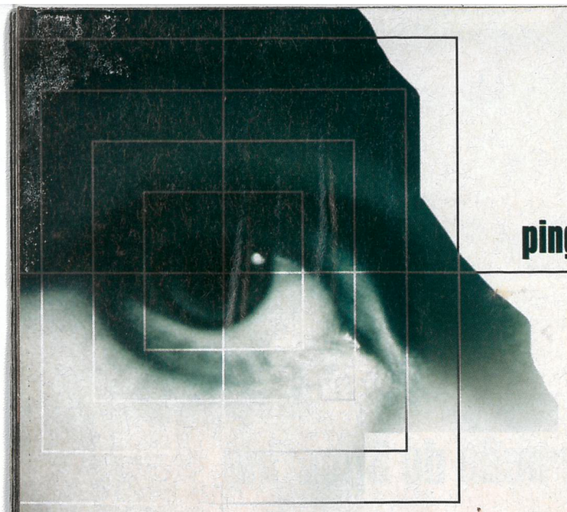
512 - rexec
513 - rlogin
514 - rsh

Pode-se fazer essa varredura com o Nmap que está no CD da revista.

A sintaxe para utilização da varredura é:
Nmap -O -p512-515
IP_DA_MAQINA

Após o parâmetro -p, informe a porta a ser verificada. Já o parâmetro -O identifica o sistema operacional da máquina-alvo. Se for Windows, o IP não será usado neste método de ataque. Certamente não será possível realizar o spoofing através desta máquina. Um raro caso onde o Windows é mais seguro. No caso de computadores que rodam Linux, ele identifica (com sucesso, na maioria das vezes) até mesmo a versão do kernel que está em operação.

No entanto um servidor bem configurado certamente irá identificar o IP de uma suposta invasão durante esse processo. Para evitar que isto aconteça, os hackers costuman usar os parâmetros -f durante o uso do nmap, de forma que o cabeçalho do endereço IP e os pacotes venham fragmentados, o que pode ser muito útil para que o hacker passe despercebido na hora de analisar um sistema.



Tipos de Ataque

Os tipos de ataque que utilizam a técnica de spoofing mais conhecidos são:

IP Spoofing
ARP Spoofing
DNS Spoofing

- ARP Spoofing

Esta técnica é uma variação do ip spoofing, que se aproveita do mesmo tipo de vulnerabilidade, diferenciando apenas porque se faz na autenticação ARP, apesar de também ser address-based utiliza o endereço MAC (Media Access Control) ou o endereço físico do dispositivo, geralmente uma placa de rede.

DNS Spoofing

Técnica muito simples, não requer grandes conhecimentos do TCP/IP. Consiste em alterar as tabelas de mapeamento de hostname-ipaddress dos servidores DNS, ou seja, seus registros do tipo host (1), de maneira que os servidores, ao serem perguntados pelos seus clientes sobre um hostname qualquer, informem o ip errado, ou seja, o do host que está aplicando o DNS spoofing.

Como a máquina-alvo é derrubada

Primeiramente precisa-se derrubar a máquina-alvo.

Isso pode ser feito através de várias maneiras, mas uma das mais utilizadas é o Dos (Denial of Sevice - Negação de Serviços). Este método consiste em sobrecarregar o computador-alvo até que ele pare de responder. Por incrível que pareça esta é a parte mais complicada de todo o procedimento de spoofing. Uma vez que a máquina-alvo for retirada do ar fica fácil assumir seu endereço IP.

Uma das utilizações do Dos mais utilizadas é o smurf, esta técnica o invasor envia uma solicitação de ping em broadcast para a rede que será atacada. Nesse caso o que vale mesmo é a largura de banda, que precisa ser maior do que a da máquina-alvo. Por esse motivo, dificilmente um smurf parte de um único computador. Geralmente este procedimento necessita de um grupo de atacantes para concretizar a derrubada da máquina-alvo. Nem sempre um invasor dispõe de tanta ajuda assim para realizar um ataque.

Outra técnica muito utilizada é o ataque pelo protocolo ICMP, que possui a vantagem em relação aos outros de não é necessário nenhum tipo de programação complexa. Através do Linux, em modo texto, é possível tirar uma máquina do ar com linha de comando:

ping-t-l 1024 ENDEREÇO_IP

O ATAQUE

A etapa mais difícil de ser realizada é a derrubada do alvo, uma vez que o IP da estação-alvo parar de responder, é só rodar um programa que muda o endereço de sua requisição. Um exmplo desse tipo de software é o Hijack, que também está no CD-ROM é só você copiá-lo para o seu Linux.

Monte a sua unidade de CR-ROM e digite o comando:

```
cp
/mtm/cdrom/linux/Spoofing/hijack.c
/root/
```

Depois de copiar o arquivo, o próximo passo será compilar o programa.

É necessário que você tenha um compilador C (como o gcc, por exemplo) instalado em seu Linux. Confira agora como compilar:

```
gcc -o hijack hijack.c
```

Depois de fazer experiências de teste com o Hijack, use o comando:

hijack host_confiável 23 endereco_alvo

Neste caso, o host_confiável nada mais é do que o endereço que foi derrubado.

Já o número 23, que aparece logo em seguida, é a porta de Telnet. Ela é necessária para que o IPSoopofing seja realizada com sucesso. Por fim o endereço-alvo é o IP do computador que será invadido.

Sendo assim, tudo o que um invasor precisa fazer é alterar as configurações deste comando para os dados referentes a máquina-alvo, e pronto: o spoofing está feito.

COMO SE PROTEGER

O procedimento de IPSpoofing é bastante complexo e pode causar muitos problemas aos administradores de sistema. Por isso é altamente recomendável que você proteja a sua rede antes que ocorra algum ataque.

Não existe uma solução definitiva que proteja esse tipo de ataquepois o IPSoopofing é uma característica do TCP/IP. Tudo o que ela faz é se utilizar dos recursos deste protocolo e enganar a máquina com o qual o invasor está realizando a troca de pacotes. Podemos mencionar duas soluções que podem ser muito úteis para que isso não aconteça. A primeira delas é não utilizar os serviços rexec, rlogin e rsh, exceto se eles forem extremamente necessários. Esses serviços geralmente não são utilizados, pois facilitam invasões. Se esses serviços realmente sejam necessários, implante uma política de segurança eficiente com o auxílio de uma ferramenta criada especificamente por esse propósito, as IDS (Instrusion Detection System - Sistema de Detecção de Intrusos). Você pode saber mais sobre estes sistemas no site www.snort.org.

LINKS PARA UTILITÁRIOS DE SPOOFING

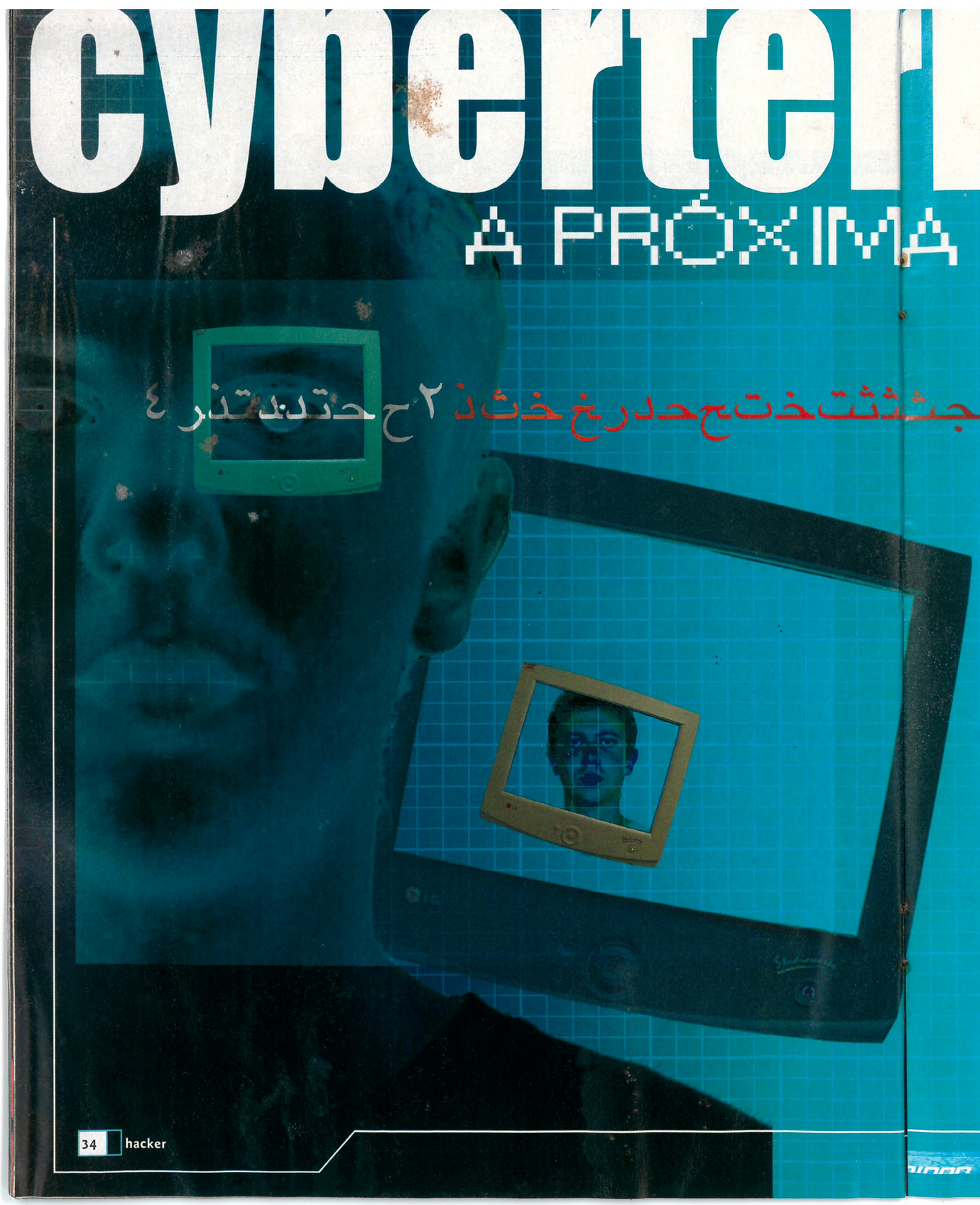
http://insecure.org/sploits/ttcp.spoofing.problem.html
http://lin.fsdi.cvut.cz/~kra/index.html
www.net-security.sk/network/spoof/rbone.tar.gz
www.deter.com/unix/software/arnup.cwww.deter.com/unix/
http://all.net/journal/netsec/9606.html

Kevin Mitnick

O ataque por spoof ficou famoso a partir de dezembro de 1994, apesar de ser uma técnica conheceida desde 1989. Tsutomu Shimomura, famoso especialista em segurança que trabalhava para a San Diego Supercomputer Center, teve seus computadores pessoais invadidos pelo hacker Kevin Mitnick.

cyberterrorismo

A PRÓXIMA AMEAÇA



Terrorismo é definido como o uso de práticas ilegais contra pessoas ou propriedades para intimidar ou coagir um governo, a população civil, ou qualquer segmento, em prol de objetivos políticos ou sociais. Assim diz a polícia federal norte-americana, o FBI (www.fbi.gov).

Esses métodos vêm sendo utilizados há muitos anos, principalmente na Europa, por grupos separatistas como o basco ETA, o irlândes IRA e, em nosso país, por políticos de mau-caráter. Mas os ataques aos Estados Unidos, no dia 11 de setembro, foram o expoente máximo das práticas terroristas, devido à ousadia de seus idealizadores e ao impacto causado pelas imagens exibidas na televisão. Nada será como antes. O medo de novos atentados e de retaliação estará presente na mente de todos. A qualquer momento, um carro-bomba poderá explodir em frente a uma embaixada; alguém poderá receber uma carta contendo um pó letal; aviões poderão se chocar contra monumentos; bombas nucleares poderão ser detonadas à distância etc.

Mas em uma sociedade que tem crescido e se desenvolvido apoiada na tecnologia, nas facilidades das transações on-line e na rapidez na troca de informações, não se pode pensar apenas na destruição física do que se conhece. É preciso levar em conta também a ameaça de ataques e da destruição digital: o "cyberterrorismo".

Criado na década de 80, por Barry Collin, pesquisador do Instituto de Segurança e Inteligência da Califórnia (www.sans.org), o termo define a nova cara do terrorismo, agora praticado no mundo virtual. Em texto de 1997, Collin descreve três possíveis casos de cyberterrorismo: no primeiro, um cyberterrorista entra nos computadores que controlam a produção de uma indústria de cereais e altera a dosagem de ferro utilizada. Milhares de crianças adoecem e morrem. Ou então, ataca os sistemas de controle de tráfego aéreo de um aeroporto.

Dois aviões colidem (hum... já vi esse filme). Por último, a economia mundial é abalada por interferências nas transações bancárias e na cotação dos papéis das bolsas de valores. A população fica temerosa e o sistema financeiro entra em colapso. Tudo executado remotamente a milhares de quilômetros de distância.

Caótico? Essa é a intenção. Impossível? Já percebemos que não.

cyberterrorismo

Recentes estudos feitos pelo governo dos Estados Unidos comprovaram a fragilidade dos sistemas de computadores dos órgãos públicos e das redes de comunicação do país. Imagina-se que um ataque eletrônico possa causar mais danos do que uma investida militar.

Ferramentas e prevenção

Basicamente, os cyberterroristas se utilizam de falhas ou configurações erradas em softwares. Esses bugs permitem acesso - às vezes, privilegiado - ao sitema de arquivos da empresa, deixando-a à mercê do invasor. Outras formas de ataque comuns são o mail bombing e os DoS (Denial of Service), que podem tirar uma rede do ar por horas, através de excessivas solicitações de serviço.

O combate a ataques cibernéticos ainda é difícil, pois muitas empresas não têm estrutura e nem planos estratégicos para detectá-los e combatê-los. Estes planos incluem a caracterização das intenções do 'inimigo', suas técnicas de atuação, recursos e agentes. Algumas empresas também omitem as invasões, visando evitar a exposição de seus problemas na mídia.

A solução é investir em tecnologia. Firewalls, equipamentos mais seguros e atualizações (patches) de programas são lançados a todo momento e para todos os perfis. Segundo a Intersix Technologies (www.intersix.com.br), companhia líder no mercado nacional no fornecimento de sistemas para segurança de informação, o aumento no volume de negócios no mês de outubro foi de 40%. Crescimento relacionado aos eventos de 11 de setembro que mostra a preocupação das corporações com a vulnerabilidade de seus dados.

Essa preocupação também se reflete na esfera legal. No dia 18 de outubro, o governo brasileiro publicou o decreto número 3.976. Nele são instituídas medidas de repressão ao terrorismo por meio de ações como o controle e a segurança das informações. Essa prevenção tem por base a investigação e repressão por parte dos governos, o bloqueio à captação de fundos e o congelamento de recursos financeiros de grupos ligados direta ou indiretamente ao terrorismo. Nos EUA, a nova lei antiterror prevê a prisão perpétua sem direito à fiança, como acontece, hoje em dia, aos atos terroristas, para os cyberterroristas.

O hacker e o cyberterrorismo

Uma questão surge em meio a essa discussão: o hacker é um terrorista? Para os mais conservadores, os dois se confundem, mas existem algumas diferenças entre eles. Na verdade, é preciso colocar um terceiro personagem na história: o cracker.

O hacker é aquele sujeito curioso que gosta de computadores. Ele fica feliz ao aprender uma nova técnica de programação ou ao descobrir uma brecha naquele programa recém-lançado. Não é nenhum anjo, mas não se sente tão recompensado ao invadir e derrubar um site movimentado, coisa que levaria um cracker a dar pulos de alegria. Esta é a principal diferença entre os dois: um fuça, enquanto o outro invade. Mas ambos por razões pessoais, nada de ativismo.

Vem agora o terrorista. Este alia as ferramentas do hacker e o espírito de desafio do cracker a motivações políticas e sociais.

A mídia, em geral, não avalia esta diferença. Jornais, revistas, TV e cinema fazem dos três uma pessoa só. E uma pessoa criminosa. Mas na guerra contra o "terror", os hackers têm sido muito importantes. Foram eles, por exemplo, que entregaram ao FBI informações sobre as contas bancárias de Bin Laden e rastrearam as movimentações de dinheiro de sua organização, a Al Qaeda. Um desses grupos é o fundado pelo milionário e ex-hacker alemão Kim "Kimble" Schmitz, o Yihat - Jovens Hackers Inteligentes Contra o Terror (www.kill.net). Contando com mais de 9.000 membros, em 2 meses de fundação, ele reuniu tantas informações que agora partiu para uma segunda fase de atuação, fechada ao público e destinada apenas a monitorar atividades terroristas.

Projetos como esse ajudam a mudar a imagem que se tem do hacker, mostrando o lado da sua consciência social. Como grande conhecedor da área de informática, ele pode apoiar a sociedade em atos de repúdio a brutalidades como as do dia 11 de setembro - sem cometer excessos, é claro.

e-Jihad

Enquanto aliados e mulçumanos se enfrentam por céu e por terra, a guerra santa eletrônica também se desenrola. Grupos de hackers que apoiam o Taleban e Osama Bin Laden, ou que querem simplesmente aparecer, já começaram a atacar sites relacionados ao governo dos Estados Unidos. O site da Administração Atmosférica e Oceanográfica Nacional : (www.noaa.gov), responsável pela previsão das alterações climáticas no planeta, foi vítima de um ataque em novembro de 2001. Os invasores - um conhecido grupo paquistanês chamado GForce - deixaram graffiti político e deixaram o site fora do ar por algumas horas, mas nenhuma informação ou equipamento foi danificado.

O GForce tem desempenhado papel de destaque na união de forças contra os E.U.A., e já anunciou que continuará atacando sites militares e de aliados americanos (http://www.nipc.gov).

- Saiba Mais:

www.terrorism.com
www.newsfactor.com
www.terrorism.com
www.cyberarmy.com
www.cracker.com
www.securityfocus.com

ESPECIAL

COUNTER-STRIKE
UM MOD ANTITERRORISMO PARA O HALF-LIFE

Counter Strike é mais um game primeira pessoa, virou febre nas Lan-Houses aqui de São Paulo, que por sinal tem crescido muito ultimamente, não só aqui, mas em todo país. Counter Strike explodiu de forma assustadora. Atrai cada vez mais adeptos, de todas as idades. CS se trata de um jogo, onde terrorista e contra-terroristas travam combates serrados para concluírem seus objetivos. O que se destaca mais é o espírito de equipe, que afinal é indispensável no jogo. Mais de 25 armas estão à sua disposição no jogo, entre elas escopetas, submetralhadoras, rifles, granadas e claro os equipamentos indispensáveis como o colete e o capacete, que com certeza aumentam suas chances de permanecer vivo por mais tempo no combate. Há armas para todos os estilos de jogadores, os que gostam de "Campear", mais conhecidos como Campers, os que gostam de ir cara a cara pro combate, os estratégicos... Enfim, você saberá qual a melhor arma para utilizar experimentando todos os tipos, nem sempre a mais cara ou a mais chamativa são as melhores, a melhor arma é aquela com a qual você mais se adaptar. Muitas pessoas reclamam de CS, pelo fato de não ter a opção Single Player, a opção de jogar sozinho, mas isso será resolvido, em nossas próximas edições faremos uma matéria sobre Counter Strike - Condition Zero, que é a versão Single Player do mesmo, mais um lançamento da Valve (produtora de Half-Life) mas enquanto isso, saiba um pouco mais sobre CS, o MOD mais famoso de Half-Life. Os MODs deixaram de ser somente um hobby e ganharam a atenção de toda a indústria com o surgimento de Counter-Strike, em 1999. Baseado no já excelente Half-life, sem dúvida um dos melhores jogos para PC de 1998, para

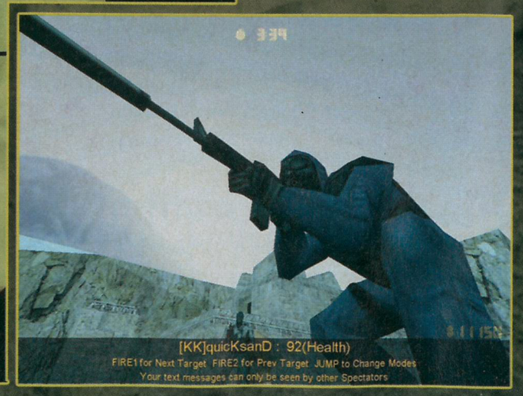
"Mais de 25 armas estão à sua disposição no jogo, entre elas escopetas, submetralhadoras, rifles..."

alguns superando até a linha Quake, que é o pioneiro na categoria. CS substitui a atmosfera de ficção científica daquele jogo por um tema militar, abordando um tema altamente realista. Counter-Strike simula o confronto entre um grupo terrorista e uma equipe de contra-terroristas, nas mais diferentes missões: Armação de bombas C4, assassinato de VIPs, fuga, resgate de reféns ou simplesmente combate homem a homem, ou grupo a grupo. O segredo do jogo está na mistura perfeita de estratégias para cada uma das facções existentes, cenários e armas que reproduzem perfeitamente seus modelos reais e a ação típica dos jogos de tiro em primeira pessoa no estilo Quake. Mas existem muitos fatores que fazem de Counter Strike o melhor e mais bem sucedido MOD dos últimos tempos, tudo é muito bem calculado no jogo, por exemplo, quando você está andando com uma arma pesada, sua mobilidade diminui bastante, os movimentos de recarga das armas são perfeitos, cada arma tem um tipo de recarregamento, isso é óbvio, mas o movimento das mãos do personagem para cada um desses tipos, é perfeito, tem armas com recarregamento rápido, umas com recarreganto lento. Saiba quais as melhores armas, nas fichas técnicas de todas as armas do jogo, que você encontrará nas próximas páginas. Outro ponto a favor de CS são as constantes atualizações feitas no jogo, uma característica comum dos MODs. Diferente dos jogos comerciais, que precisam obrigatóriamente obedecer um prazo de produção e de lançamento, os programadores por hobby, raramente estão satisfeitos com seu trabalho ou senão dão por terminado. Um ano depois de seu lançamento, em 1999, o jogo foi considerado pronto para sair da fase de teste e recebeu uma nova versão, que vem sendo avaliada pelos

"O segredo do jogo está na mistura perfeita de estratégias para cada uma das facções"

jogadores. Counter Strike trata-se de um título que se renova freqüentemente. Counter Strike é um dos melhores MODs com efeitos 3D bem reais; o responsável por essa façanha é o programador Canadense Mihn "Gooseman" Lee. Também conhecido por colaborar com outros bons jogos de ação e partiu para um novo projeto por gostar de jogos realistas de ação e tática. Com softwares conhecidos, como o 3D Studio Max, para modelagem 3D (o melhor da categoria atualmente), e copiando o áudio de filmes para obter os sons das armas, Gooseman não fazia idéia do impacto e do sucesso que CS teria. Feito especialmente para ser jogado sempre entre dois times, CS conquistou rapidamente o público mais exigente com gráficos e sons quase perfeitos e reais. Este jogo está tão bem-sucedido que os jogadores deste MOD superam com grande facilidade os jogadores de Quake III Arena e Unreal Tournament, que por sinal são excelentes jogos, isso pode ser comprovado nas Lan-Houses, entre em qualquer uma Lan-House com mais de 20 pessoas jogando e veja quantos estão jogando Counter-Strike e quantos estão jogando algum outro jogo. Gooseman e seus colaboradores comentam a possibilidade de um Counter Strike 2. O sucesso deste jogo conseguiu grande feitos, que impulsionaram o bom dos jogos de ações táticas, foi lançado comercialmente pela Valve, e vai render sua própria expansão, Condition Zero, que é um CS com missões para um único jogador (como citado acima). CS inspirou diversos outros títulos, que começaram a surgir em todas as plataformas possíveis. Esperamos bons lançamentos de títulos nessa categoria, pois para quem gosta, isso só tende a aumentar e a melhorar.

"BOMB HAS BEEN PLANTED"



■ Distribuidor: **SIERRA** ■ Fabricante: **VALVE INTERACTIVE** ■ Origem: **ESTADOS UNIDOS**
■ Requisitos de sistema: Pentium III 600Mhz, 64 MB RAM, Placa de vídeo 3D, 400Mb de espaço livre no HD

SHOOTER

UNREAL TOURNAMENT 2003

INFOGRAMES MOSTRA O QUE É UM VERDADEIRO GAME VIOLENTO

Definitivamente o ano 2002 será sempre lembrado como o ano dos jogos de ação. Quando já estávamos muito ocupados com o anúncio dos lançamentos dos jogos Unreal 2, Soldier of Fortune 2, Allied Assault, Serious Sam 2, eis que a Infogrames anuncia inesperadamente o início do desenvolvimento do melhor jogo de ação dos últimos tempos, Unreal Tournament. É muita adrenalina.

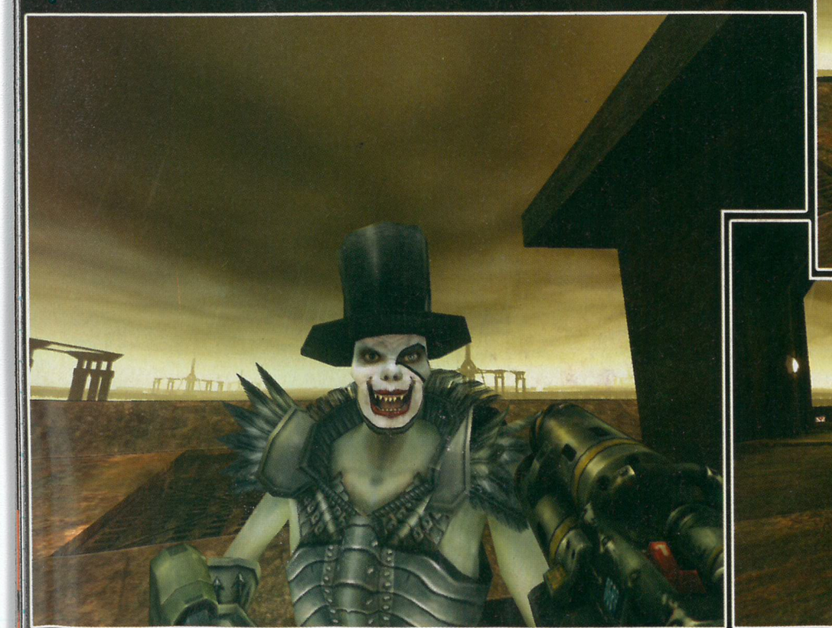
UM VERDADEIRO TORNEIO

Desde que foi lançado, Unreal Tournament destacou-se desde logo da sua concorrência. Com um sistema multiplayer fabuloso, este jogo desde logo reuniu uma forte comunidade de jogadores online. Não é por acaso que foi automaticamente inserido nos World CyberGames (Lan-Houses), sendo desde então, um dos jogos de ação, mais completos de todos os tempos. Unreal Tournament 2 pretende ocupar este lugar de destaque. Esta segunda edição terá 30 arenas diferentes, mais de 50 personagens, totalmente personalizados, uma enorme quantidade de armas e 5 modos multiplayer, completamente novos. Uma das maiores inovações virá do seu modo de um só jogador, que segundo os seus programadores, será muito diferente do primeiro jogo. Foram incluídos movimentos especiais, que permitem tornar o jogo mais dinâmico. Estes movimentos especiais vão depender da sua bioenergia, que pode ser colecionada e que permite gravar mais de três destes movimentos.

Algumas armas foram alteradas, foi reduzido o spam de algumas e podemos dizer que o impacto de algumas destas armas é bem real. Os gráficos mostrados neste game é basicamente o mesmo do Unreal II e segundo os seus programadores, é muito poderoso. Mas todas estas inovações têm um preço a pagar, por isso não esperem que este jogo rode num simples computador. Unreal Tournament 2 foi desenvolvido para funcionar em sua totalidade em computadores com pelo menos um processador acima de 1GHz e 256MB de RAM. Os cinco modos multiplayer são inovadores, oferecendo uma nova forma de jogar online. Capture the Flag e Deathmatch são dois modos que vieram do jogo anterior, mas que contêm algumas inovações. Domination 2 permite uma luta titânica entre duas equipes, na busca da conquista de dois pontos estratégicos. Bombing run é talvez o modo considerado mais difícil entre os jogadores (devido às possíveis estratégias em grupo).

"Domination 2 permite uma luta titânica entre duas equipes, na busca da conquista de dois pontos estratégicos."

Imaginem ter que pegar numa bomba e colocá-la na base da equipe adversária. Team Deathmatch é o quinto modo multiplayer de Unreal Tournament 2 e como o nome indica, é uma luta entre duas equipes. Agora vamos falar um pouco desse ótimo lançamento da Infogrames. O menu tem as seguintes opções: single player: inicia uma nova partida onde você vai passar por diversos mapas até chegar ao objetivo final; coop league: liga em modo cooperativo; multi player: jogo online; instant action: ação imediata, escolha um modo de jogo e um mapa; settings: definições de controles, som, vídeo e rede; databanks: informações variadas sobre os planetas e raças que



CHACINA

aparecem no jogo. Trouxemos também informações importantes sobre os mapas desse lançamento.

Os mapas são quase todos maiores que os do Unreal Tournament, a lista de mapas são: Deathmatch / Team Deathmatch, Vidona, Antalus, Flux, LeviathanB/Gael, TokaraForest, Compressed, Asbestos, Insidious, Inferno, Gestalt, Curse; Capture The Flag, Chrome, LostFaith, LavaGiant, Kretzig, Lethargic, Maul, Orbital; Double Domination, Core, TempleAnubis, Outrigger, Ixcorra; Bombing run, Kelandra, ElectricFields. Ainda não está confirmado o número exato de mapas, esses são apenas alguns dos que virão, porque no mínimo serão 6 mapas para cada modo de jogo, 1 mapa para cada raça. Agora vamos ao que interessa, armas. As armas serão quase as mesmas do Unreal Tournament, não estará presente a GES BioRifle nem o Ripper, todas as outras foram modificadas e foi adicionado o Ion Cannon, outra arma de destruição maciça como a Redeemer que também estará presente. A Enforcer foi substituída pela Assault Rifle, com uma velocidade de disparo grande e com a possibilidade de lançar granadas no segundo tiro. O Impact Hammer também conhecido por Piston, existindo agora uma barra que mede a intensidade da porrada, muito útil para se efetuar "hammer jump", o segundo tiro é um shield que o protege dos tiros adversários durante algum tempo. O Translocator, utilizado nos mapas de Capture The Flag e Domination (agora Double Domination) tem um sistema de utilização diferente, agora você pode fazer 5 "translocations". Tem também a Link Gun, que é idêntica a Pulse Gun, mas com a possibilidade de ligar até 3 raios para criar um "super-raio", que é guiado pela primeira pessoa que disparou, além disso o primeiro tiro está um pouco lento e mais poderoso, a Minigun continua igual. P O Flak Cannon é a arma mais impressionante, o primeiro tiro envia as mesmas 9 peças de metal, mas agora é disparado com muito mais potência. Ainda existem várias armas disponíveis neste game e com certeza falaremos sobre elas na próxima edição.

■Distribuidor: **INFOGRAMES** ■ Fabricante: **EPIC INTERACTIVE** ■ Origem: **ESTADOS UNIDOS**
■Requisitos de sistema: Pentium II 450Mhz, 128 MB RAM, Placa de vídeo 3D, 700Mb de espaço livre no HD

WEB BUGS & SPYWARE

OS PIXELS ESPIÕES

Houve uma época em que eram constantes os protestos contra o uso da internet, no entanto, o e-businnes constitui-se uma prática em grande expansão e tem determinado os padrões de comportamento dos consumidores pelas empresas vendedoras que mesmo sem permissão prévia invadem os sistemas e a privacidade do usuário com o intuito de "empurrar" seus produtos. Os artifícios de espionagem são sofisticados e sutis, como os spywave e os web bugs e não mais os inocentes cookies.

Para quem não sabe um Web bug é uma imagem muito pequena (geralmente 1 pixel) e invisível que, uma vez colocada nas páginas da web, tem a capacidade de rastrear a navegação de um internauta. Existem alguns sites que usam imagens invisíveis, isto é, com cor é exatamente igual à da página em que se encontram. Isto é para que todos os gráficos vistos pelos navegadores apresentem uma posição correta. À primeira vista os web bugs são uma imagem comum só que estes podem conter códigos HTML embutidos. E estes códigos são usados exatamente para coletar informações sobre os internautas e seus hábitos de navegação.

Quando uma página da web é visitada, o navegador solicita de vários servidores, as imagens, textos, quadros, avisos etc, que compõem a página. Em contra-partida, este envia dados sobre a máquina em que se encontram instalados. Por sua vez, os códigos HTML dos web bugs especulam dados como: endereço IP do computador a quem pertence a página em que o web bug está inserido tempo em que a página ficou aberta, hora e dia do registro do windows, navegador usado etc.

Estes dados podem ser enviados para os servidores de companhias como: Double click, Hatchlogic, Engage Technologies entre outras que as vendem às empresas veiculadoras de publicidade.

Os web bugs interagindo com os cookies, aumentam sua atuação tornando-o ainda mais suscetível de espionagem.

Há alguma forma de impedir isso? Sim, destruindoo navegador da função de baixar todo e qualquer gráfico. Mas não se esqueça de que os web bugs podem ser inseridos em qualquer programa que aceite o código HTML. Como Word, e-mail, ICQ e outros. E nestes casos é muito difícil se livrar deles.

Nem tudo está perdido, pois proporcionalmente ao avanço de meios obscuros de marketing, cresce o número de exigência dos direitos do consumidor. Exemplo disso, e que algumas pessoas já até enviaram reinvindicações sobre os web bugs às maiores companhias de publicidade eletrônica.

Para saber mais :www.tiac.net/users/smithis/privacy/wbfaq.html

VOCÊ USA O KAAZA?

Se utiliza este software para partilhar música, provavelmente terá spyware instalado no seu computador. A aplicação chama-se B3D Projector e foi escrita pela Brilliant Digital. Pode usar Add/Remove Programs para remover o B3D Projector, mas este deixa uma série de arquivos atrás de si. Uma vez removido, termine a tarefa procurando e apagando os seguintes arquivos: bdeinstall.exe, bdeinsta2.dll, bdefdi.dll, bdedata2.dll, bdedownloader.dll, bdeverify.dll, bdesecureinstall.exe and bdesecureinstall.

De seguida, corra o Regedit e apague as entradas 'b3d' (se as encontrar) nas duas chaves seguintes:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\currentVersion\Run\
HKEY_CLASSES_ROOT\Software\ZUpdata

Dicas de remoção

• O Newdotnet é um plug-in para o IE que é instalado por uma vasta gama de software, principalmente aplicações de partilha de arquivos. Podemos removê-lo através da opção Add/Remove Programs do Control Panel. No entanto, deve verificar se não deixou quaisquer controles Activex. No IE vá a Tools, Internet Options, Temporary Internet Files, Settings, View Objects e apague tldctlz.

• O ClickTheButton (Ctbclick.exe) instala-se automaticamente a si mesmo. Para o remover é necessário apagar CTB3_Shared do diretório Windows e apagar CTBHooks.dll no diretório System (Windows\System ou Windows\System32).

• Será também necessário editar o Registry. Vá em:
HKEY_LOCAL_MACHINE\SOFTWARE\
e apague a chave CTB_BrandedClient.
Depois, vá em:
HKEY_LOCAL_MACHINE\
SOFTWARE\Microsoft\Windows\
CurrentVersion\Run e apague a chave ClickTheButton.

• Em http://accs-net.com/smallfish/gohip.htm encontra instruções para a remoção de Gohip.com.

• O Gearbox Connection Kit, da RockstarSoftware, é usado por alguns ISP para permitir a configuração ou a atualização automática dos ajustes de conexão dos utilizadores. Em alguns casos, estes alteram a página principal. Encontra instruções de remoção em www.cexx.org/gearfix.txt.

• O www.ezcybersearch.com pode ser instalado visitando a respectiva homepage em:
www.ezcybersearch.com/uninstall.html.

• O Lop.com apodera-se da sua página principal, mas proporciona um desinstalador em http://lop.com/uninstall.exe.

• O B3D Killer procura e erradica as entradas da Brilliant Digital existentes no seu sistema em:
www.wilderssecurity.com/B3DKiller.html.

MUNDO DIGITAL
preserve seus dados

VERSÃO BETA DO GOOGLE ENTRA NO AR

No dia 23 de setembro entrou no ar, ainda em versão beta, o Google News - um novo serviço do portal de busca que tem como missão centralizar as principais notícias do dia dadas por cerca de quatro mil veículos online. O serviço irá beneficiar quem quer estar informado sobre o que acontece no mundo e não tem tempo de ficar entrando em todos os sites de notícia para procurar o que é mais interessante. Está quase tudo em um lugar só, e a cobertura é bastante ampla - tem The New York Times, BBC, Fox News, Business Week, Zdenet, Yahoo!Headlines, Smart Money, Canada.com e uma série de jornais regionais das mais diversas localidades do mundo. No catálogo, estão as notícias publicadas nos últimos 30 dias. Com atualizações automatizadas diárias divididas em sete editorias (Mundo, Estados Unidos, Negócios, Ciência e Tecnologia, Esportes, Entretenimento e Saúde), o Google News possui um sistema que avisa há quanto tempo a notícia original foi colocada no ar e há quanto tempo o site foi atualizado - você entra na home do serviço e pode visualizar, no topo à direita, uma frase que diz "esta página foi gerada há "tantos minutos". Quem quiser pode optar por organizar as matérias cronológicamente. As principais notícias são acompanhadas por fotos e links para a mesma informação dada por outros sites, para que você possa optar pelo veículo que lhe interessar mais. A escolha da disposição das mesmas na home é randômica, por meio de algoritmos, sem edição humana - aliás, não foi contratado nenhum funcionário para este novo serviço, segundo a Google. A empresa diz que, assim, o usuário pode acessar notícias com opiniões divergentes e até mesmo informações contraditórias em um mesmo bloco, compondo uma forma mais abrangente de se manter informado. A Google promete que ainda fará melhorias na página e cadastrará um número maior de veículos. Vale a pena conferir! http://news.google.com.

Furo de segurança no Flash afeta Windows e Linux

Um furo de segurança no tão conhecido formato de arquivo, Macromedia Shockwave Flash, usado em browsers web, permite que o atacante execute código de sua escolha nos sistemas afetados, de acordo com um novo alerta de segurança lançado pela eEye Digital Security. A vulnerabilidade é limitada, porém, aos arquivos Shockwave Flash editados manualmente com um editor binário, sendo que a aplicação Flash não produzirá arquivos que contém vulnerabilidade por próprio, de acordo com um altera de segurança separado da Macromedia. A vulnerabilidade é séria pois afeta browsers web. O furo vem como resultado de um problema no cabeçalho de dados dos arquivos Shockwave Flash que permite ao atacante fornecer mais dados ao decodificador do arquivo do que o esperado e pode eventualmente direcionar à execução do código. A Macromedia lançou uma nova versão do Flash player que corrige o problema e está disponível no seguinte endereço:http://www.macromedia.com/v1/handlers/index.cfm?ID=23293&Method=Full&TitlePSB02%2D09%20%2D%20Macromedia%20Flash%20Malformed%20Header%20Vulnerability%20Issue&Cache=False. A eEye, que encontrou outras numerosas vulnerabilidades em aplicações como IIS (Internet Information Services), descobriu outro furo de segurança no Flash em maio. Mais relatórios de bugs devem seguir-se, pois a eEye avisou em seu alerta que encontrou outras 17 vulnerabilidades no Flash.

Quem sou eu? De onde vim?

Muitas pessoas ainda não sabem a origem de seus ancestrais e morrem de curiosidade de saber se são realmente italianos, indios etc. Se você tem curiosidade sobre sua árvore genealógica, ficou bem mais fácil fazer pela internet. Sites completos revelam origens de sobrenomes e ajudam você a combinar informações. Confira a seguir algumas páginas brasileiras e internacionais, que ajudam na pesquisa de seus ancestrais. Brasileiros: www.genealogia.com.br, www.imigrantesitalianos.com.br, www.gentree.org.br, www.memorialdoimigrante.sp.gov.br, www.auxilio-a-lista.com.br; Internacionais: www.familysearch.org, www.rootsweb.com, www.ancestry.com, www.ellisisland.org www.genealogy.com

Primeiro "smiley" completa 20 anos em setembro

Um pesquisador da Microsoft descobriu a origem dos primeiro "smiley" computadorizado. Desde sua primeira aparição, em um boletim eletrônico da Carnegie Mellon University, em setembro de 1982, o smiley deu origem a uma série de outras expressões faciais que ganharam o nome de emoticons. Smiley foi o nome dado àquela combinação de caracetres — :-) — que forma uma carinha sorrindo em mensagens computadorizadas. A partir daí, os emoticons ganharam um papel importante na cultura social on-line porque eles facilitam a comunicação rápida de expressões —algo complicado de se conseguir expressar por palavras. Mike Jones, pesquisador do grupo de estudos de sistemas e redes da Microsoft, deu início à busca do primeiro smiley em fevereiro deste ano, segundo publicado pelo News.com. Em um site, Jones diz que muitas pessoas estariam envolvidas na busca pelo primeiro smiley. "Eu dei início ao esforço...procurando em fontes de antigos boletins eletrônicos", disse Jones. Ele se lembrava de ter visto um boletim da Carnegie Mellon University com esses caracteres no início da década de 80. Com a ajuda de Howard Wactlar, um ex-diretor da faculdade de ciências da computação da Carnegie Mellon, e de Bob Cosgrove, atual diretor, Jones encontrou a fita de backup de todos os arquivos usados entre 1981 e 1983. A fita teve que ser restaurada e muitas pessoas procuraram pelos documentos até encontrar o smiley. O primeiro uso dos caracteres :-) significando um sorriso, segundo acredita Jones, foi feito em 19 de setembro de 1982, por Scott E. Fahlman. "Proponho usar a seguinte combinação de caracteres para sinalizar piadas: :-)", teria escrito Fahlman naquela época. "Leia os sinais de lado. Na verdade, talvez seja mais prático marcar as coisas que não são piadas, dada a atual tendência. Para isso, use :-(. "O dia 19 de setembro poderia juntar-se a outras datas significativas para a revolução da informação. A internet foi criada 13 anos antes disso e o e-mail, em 1971. Bem como a internet, o e-mail não tem uma data específica de surgimento. Ray Tomlinson, engenheiro americano considerado o "pai do e-mail", não sabe dizer quando a primeira mensagem foi enviada, para quem ou o que ela dizia. Tomlinson teve muito trabalho com os já existentes métodos de troca de dados e criou caixas de mensagens remotas, capazes de enviar e receber mensagens por uma rede de computadores. Além disso, designou o hoje famoso símbolo "@" para assegurar que uma mensagem fosse enviada um determinado destinatário.

eDonkey

O eDonkey é uma interessante mistura de Napster com Gnutella. Dividido em cliente e servidor, não depende de um servidor central. Compartilha qualquer tipo de arquivos, e tem busca bem rápida e eficiente. Versão GUI (Graphical User Interface). Com o eDonkey, você poderá encontrar e disponibilizar qualquer tipo de arquivo, seja um programa, vídeo, música ou foto, não importando a extensão. Para os mais desavisados, donkey, em inglês, significa Burro.' Portanto, eDonkey eletronic Donkey) é "Burro eletrônico". Roda em Windows 95, 98, NT, 2000, ME, XP. A policia dinamarquesa fechou seis servidores da eDonkey aparentemente pressionada por um grupo antipirataria. Mas seus servidores não hospedam os arquivos ilegais (apenas organizam os dados para que a rede possa ser explorada), o que torna a ação da polícia sem precedentes. O eDonkey vem sendo considerado um dos melhores programas de compartilhamento de arquivos, então aproveite o programa contido no CD! Informações para registro: Este software é um Shareware e o registro custa US$ 20,01. Algumas opiniões: Péssimo com rede discada se leva uma eternidade pra baixar os files, e além disso os usuários de conexão rápida tipo DSL saem na vantagem pois o PC com Dial-Up fica pesado no Upload e lento no download, isso quando se consegue conectar num servidor com bastante files disponíveis... O melhor mesmo é o Kazaa Media Desktop 1.7.1, pois é bem mais rápido e não tem Spyware como os outros. (Anônimo) legal... mas complicado! é bem interessante, mas um pouco complicado. No site www.edonkeybr.cjb.net tem uma versão em português.
No site www.edonkey200.com existe um forum em portugueses. (Anônimo) Ótimo Mesmo com conexão dial-up, os servidores te deixam entrar... é possivel conectar em qualquer servidor ativo respeitando o máximo de usuários... toneladas de arquivos, vídeos e músicas, porém alguns arquivos grandes têm pedaços faltando.

Apagando seus Rastros

É possível alguém descobrir por quais sites você andou navegando? Sim, isso é possível. Por isso, se você tem um micro em casa ou no trabalho, tome muito cuidado com aqueles sites "espertos" que você anda navegando na hora do almoço, para "relaxar"... E não precisa ser nenhum Sherlock Holmes para descobrir isso: basta acessar a lista dos últimos sites visitados presente no seu browser! Mas, é claro, há como apagar os seus "rastros". O primeiro passo é você apagar a lista dos últimos sites visitados de seu browser. Se você usa o Netscape Communicator, entre no menu Editar, opção Preferências e, na opção Navigator, clique na caixa Limpar Histórico (outro caminho é através do menu Communicator, opção Ferramentas e, na opção Histórico, selecione tudo e pressione a tecla Del). Na mesma tela, clique na caixa Limpar Barra de Navegação. Já no Internet Explorer, vá até o menu Exibir, opção Opções da Internet e clique na caixa Limpar Histórico do campo Histórico. Se você é um usuário malandro, já conhece bem essa dica. Só que só isso não é o suficiente. O browser copia para o disco rígido do micro os arquivos HTML e as imagens carregados dos últimos sites que você navegou. Esse processo é conhecido como cache e serve para tornar a navegação mais rápida. Quando você entra em um site que você já tenha visitado e caso os arquivos dele estejam no disco rígido, o browser carrega os arquivos contidos no disco rígido, processo que é bem mais rápido do que ter de carregar os arquivos da Internet. Se algum bisbilhoteiro quiser saber por onde você navegou, basta uma rápida olhada no diretório do disco rígido que o browser usa como cache para ver as fotografias das mulheres em trajes sumários que você andou "pesquisando" na Internet. Dessa forma, o macete é apagar o conteúdo desse diretório após ter navegado na Internet, caso você queira que realmente ninguém saiba por onde você andou e o que você andou vendo. Isso pode ser feito de dentro do próprio broswser. No Netscape Communicator, vá ao menu Editar, opção Preferências, opção Avançado. Na opção Cache, clique sobre a caixa Limpar Cache de Disco. Já no Internet Explorer, vá até o menu Exibir, opção Opções da Internet e clique na caixa Excluir Arquivos do campo Arquivos de Internet Temporários. Esses procedimentos irão apagar todos os vestígios de sua navegação de sua máquina. Só tome cuidado, porque se você acessa a Internet através da rede da empresa que você trabalha, a rede pode estar configurada para monitorar todos os acessos à Internet. Dessa forma, mesmo que você apague todos os vestígios de seu micro, o administrador da rede tem acesso à lista de sites que você visitou. Nesse caso, se você realmente não quer que ninguém saiba por onde você navegou, o negócio é não navegar. Deixe para ver sites de mulher pelada em casa, à noite.

Vírus ou MP3?

Quase no fim do século XXI, a mídia de todo (inclusive alguns jornais do Brasil) proclamou o que seria a "evolução do MP3", um formato chamado MFK, supostamente capaz de comprimir até 3 vezes um MP3 com absoluta qualidade. Com informação de que o MFK fôra criado por um gênio japonês chamado Mafuka, usando "interpolação galciana" (bonito, não?) e toda uma alegoria de explicações técnicas, até os mais zelosos jornalistas se convenceram da "perfeição" MFK. Na verdade, o que o MFK faz é alojar o MP3 em algum lugar secreto do HD enquanto ilude o incauto usuário de que criou um arquivo .MKF, operando o milagre da compressão. Hackerismo pega-trouxa a serviço da inutilidade tecnologica. Se você não se lembra deste fato "interessante" da evolução "gaciana", incluimos no Cd o genial "compressor" para você testar e até pegar alguns amigos desatentos!

Cresce o risco do vírus BugBear

Devido ao rápido crescimento do número de contaminações, a Symantec aumentou, o grau de risco do vírus W32.Bugbear@mm de 3 para 4, numa escala de 1 a 5. Segundo a empresa, em apenas um dia, o volume de incidentes com o Bugbear saltou de 157 para 2039. O Bugbear é um invasor que combina uma série de características de outros vírus. Ele envia e-mails em massa; desativa programas de segurança (antivírus e firewalls); e funciona como programa-espião, deixando a máquina aberta a acesso externo. A correção para essa falha pode ser obtida no endereço www.infoexame.com.br/aberto/download/2315.shl. Mas isso não é tudo. O invasor tem capacidade de se propagar através de conexões de rede.

NOVO VÍRUS EXPLORA BUGS NO IE.

Acaba de ser detectado um novo vírus na rede. De origem desconhecida, o W32/Holar@MM, descoberto pela McAfee, se propaga via e-mail, MSN Messenger e compartilhamentos de rede. Segundo a empresa de segurança, o invasor chega como um anexo com a extensão PIF. O nome do arquivo é selecionado a partir do diretório Meus Documentos, do sistema infectado. O campo de assunto do e-mail contém o mesmo nome do arquivo escolhido, porém sem extensão. "A praga explora a vulnerabilidade do Internet Explorer 5.01 ou 5.5 sem SP2 da Microsoft, fazendo com o que o código viral seja carregado automaticamente, sem mesmo a execução do arquivo pelo usuário", alerta a McAfee. Quando o anexo é executado, o vírus se copia para o diretório Windows\System e cria uma chave de registro para que seja carregado na inicialização do sistema. A empresa de segurança considera o invasor de baixo risco devido ao pequeno número de registros recebidos no Brasil e no mundo. No entanto, recomenda que os produtos antivírus sejam atualizados semanalmente, além de estar configurados para proteção em arquivos compactados (Compressed Files).

Vírus se propaga por e-mail e rede local

O vírus W32/Holar@mm se propaga por e-mail, pelo MSN Messenger e ainda via drives de rede. Ele chega como anexo de e-mail e explora uma vulnerabilidade do Internet Explorer, nas versões 5.x. O anexo que traz o Holar é um arquivo PIF cujo nome é o mesmo de um nome de arquivo qualquer selecionado pelo invasor no diretório Meus Documentos. Uma vez executado, o Holar copia para o diretório de sistema os arquivos CmdServ.exe e WarIII.eml. O invasor também faz modificações no Registro do Windows para ser executado durante a inicialização do sistema. O Holar tenta se auto-enviar à lista de endereços do Outlook, aos contatos do MSN Messenger e a endereços encontrados em arquivos HTML encontrados no sistema. Se o destinatário do e-mail usa o IE 5.x sem atualizações de segurança, o vírus pode ser disparado automaticamente quando a mensagem for visualizada.

Domínio do Grupo HaxOrs Lab foi Hackeado

Uma notícia chamou a atenção dos freqüentadores dos canais Mirc. A notícia que rolava entre "/notices" dizia que o site do Grupo HaxOrs Lab tinha sido hackeado. Isso foi motivo de riso entre os outros grupos. Os mais cogitadores diziam que o domínio foi hackeado porque possuía o famoso bug que permite aos defacers deformarem o site usando o front page. Porém, isso era apenas uma fofoquinha. HaxOrs Lab é um grupo que vem ocupando o seu espaço de destaque no submundo virtual, eles foram responsáveis por um dos maiores ataques da história da Internet no Brasil! De uma só vez, eles tiraram do ar 500 sites italianos. O fato ocorreu em agosto passado. Os integrantes do grupo justificaram a ação dizendo que tudo foi feito por diversão. Eles alteraram a página inicial dos sites que tinham na sua maioria extensão ".it" que indica que os sites eram italianos. Os servidores Apaches estavam rodando no Sistema Operacional linux e constataram que eles estavam desatualizados. F0ul, líder do HaxOrs Lab declarou que o Domínio foi invadido não por falta de segurança, mas sim de um desgaste pessoal: "Nao teve nada de mais, apenas confiei na pessoa errada!! E aprendi com isso, que na net não podemos mais confiar em ninguém!!!" - E de certa forma deixa claro que haverá um retorno digno para o traidor que segundo relatos, é "um lamer do carderbr". O defacer fez questão de agredir F0ul e seu Grupo com palavras toscas e em inglês: "f0ul Suck my dick _|_". E, traduzindo outras frases, o invasor questionou e também satirisou com frases do tipo: Eu prefiro ver defaceds feitos em Windows por grupos menores a ver uma grande mentira feita em linux..." e "Diga para mim, isto representa o Brasil, isto é a elite?". Méritos tecnológicos à parte, a classe com que o Grupo HaxOrs recebeu tais provocações demonstra que o bom e velho ditado "Quem muito grita perde a razão", está corretíssimo afinal, quem ofende também não deve ser elite...

KËƒVÌN MiTÑi©K

Finalmente o grande segredo vem à tona

HACK: Como Mitnick invadiu Tsutomu Shimomura com um ataque de seqüência de IP. Parece haver até hoje, muita confusão sobre a trapaça de endereço IP e os ataques de conexão clandestina descritos pelo artigo NYT, em 23/01/95, de John Markoff e na advertência CERT CA-95:01. Estão aqui alguns detalhes técnicos da minha apresentados, em 11/01/95, na CMAD 3 em Sonoma, California. Esperançosamente isto ajudará a esclarecer todos os desentendimentos a respeito da natureza destes ataques.

Dois mecanismos de ataque diferentes foram usados. A trapaça de fonte do endereço IP e a predição da seqüência TPC de números foram usadas para obter o acesso inicial a uma estação de trabalho obsoleta (diskless quer dizer "sem disco", mas não entendi, então botei a palavra "obsoleta" no lugar) que estava sendo usada, em sua maior parte, como um terminal X. Depois que o acesso root foi obtido, uma conexão existente para outro sistema foi afetada por meio de um módulo STREAMS carregável do kernel.

Inclusas nesta nota estão partes de logs dos pacotes atuais do tcpdump gerados por esse ataque. No interesse da clareza (e brevidade!), algumas informações foram omitidas. Eu recomendo bastante os papéis e postais sobre trapaça de IP, de Steve Bellovin, onde ele descreve em mais detalhes a semântica do TCP handshake (alguém precisa traduzir "handshake" pra mim. Nunca fiz curso de inglês), assim como dá algumas sugestões de como vencer este ataque.

A configuração é a seguinte:

servidor = um SPARCstation rodando um Solaris 1 servindo meu "terminal X"

x-terminal = Um SPARCstation rodando um Solaris 1

alvo = o aparente primeiro alvo do ataque

Parece haver até hoje, muita confusão sobre a trapaça de endereço IP e os ataques de conexão clandestina descritos pelo artigo NYT, em 23/01/95, de John Markoff e na advertência CERT CA-95:01.

O ataque de trapaça de IP começou, mais ou menos, às 14:09:32 PST, em 25/12/94. As primeiras tentativas foram de toad.com (essa informação derivada do log dos pacotes):

14:09:32 toad.com# finger -l @target
14:10:21 toad.com# finger -l @server
14:10:50 toad.com# finger -l root@server
14:11:07 toad.com# finger -l @x-terminal
14:11:38 toad.com# showmount -e x-terminal
14:11:49 toad.com# rpcinfo -p x-terminal
14:12:05 toad.com# finger -l root@x-terminal (veja script no cd)

O aparente propósito dessas tentativas era determinar se poderia haver algum tipo de relacionamento de confiança nesses sistemas que poderia ser explorado por um ataque de trapaça de IP. Os números das portas fonte para o showmount e rpcinfo indicam que o atacante é root em toad.com.

Cerca de seis minutos depois, nós vemos uma cachoeira (não sei traduzir a palavra "flurry", então ficou "cachoeira" no lugar) de TCP SYNs (requisição inicial de conexão) de 130.92.6.97 para a porta 513 (login) no servidor. A finalidade desses SYNs é lotar a fila de conexão para a porta 513 no servidor com conexões "entreabertas", então ela não vai responder a qualquer nova requisição de conexão. Em particular, isso não vai gerar TCP RSTs em resposta a SYN-ACKs inexperados.

A porta 513 é também uma porta "privilegiada (< IPPORT_RESERVED), o server.login agora pode ser seguramente usado como a fonte putativa para um ataque de endereço trapaçeado no UNIX "r-services" (rsh, rlogin). 130.92.6.97 parece ser um endereço randômico (forjado) não usado (um que não gerará nenhuma resposta aos pacotes emitidos a ele). Veja todo o scrip no cd (script 01) o servidor gerou SYN-ACKs para os primeiros oito pedidos de SYN antes da fila de conexão encher-se, o servidor irá retransmitir periodicamente esses SYN-ACKs.

Nós agora vemos 20 tentativas de conexão de apollo.it.luc.edu para x-terminal.shell. O objetivo dessas tentativas é determinar o comportamento do gerador de números de seqüência TCP x-terminal. Note que os números de seqüência iniciais são incrementados por um a cada conexão, indicando que os pacotes SYN *não* estão sendo gerados pela implementação TCP do sistema. Isso resulta em RSTs convenientemente sendo gerados em resposta a cada SYN-ACK inexperado, então a fila de conexão no x-terminal não irá mais encher.

O aparente propósito dessas tentativas é determinar se poderia haver algum tipo de relacionamento de confiança nesses sistemas que poderia ser explorado por um ataque de trapaça de IP.

Note que cada pacote SYN-ACK emitido pelo x-terminal tem um número de seqüência inicial que é 128,000 maior que o anterior.

Nós agora vemos um SYN forjado (requisição de conexão), alegada pelo server.login ao x-terminal.shell. Supõe-se que esse x-terminal provavelmente confia no servidor, então o x-terminal irá fazer tudo o que o server (ou qualquer coisa mascarada como o servidor) mandar.

O x-terminal então responderá ao servidor com um SYN-ACK, deve responder em ACK para que a conexão seja aberta. Porque o servidor está ignorando os pacotes emitidos

O x-terminal então responderá ao servidor com um SYN-ACK, deve responder em ACK para que a conexão seja aberta.

ao server.login, o ACK deve ser forjado também.
Normalmente o número da seqüência do SYN-ACK é requerida em ordem para gerar um ACK válido. Entretanto, o atacante pode predizer o número da seqüência contido no SYN-ACK baseado no comportamento conhecido do gerador do número de seqüência TCP do x-terminal, e pode assim chegar ao ACK do SYN-ACK sem vê-lo.

```
14:18:36.245045 server.login > x-terminal.shell:
S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell:. ack 2024384001 win 4096 (veja script no cd)
```

A máquina da trapaça tem agora uma conexão de sentido única ao x-terminal.shell que parece ser de server.login. Isso pode manter a conexão e emitir dados, contanto que possa propriamente ACK todos os dados enviados pelo x-terminal. Isso envia o seguinte:

```
14:18:37.265404 server.login > x-terminal.shell: P 0:2(2) ack 1 win 4096
14:18:37.775872 server.login > x-terminal.shell: P 2:7(5) ack 1 win 4096
14:18:38.287404 server.login > x-terminal.shell: P 7:32(25) ack 1 win 4096
```

que corresponde a:

```
14:18:37 server# rsh x-terminal "echo + + >>/.rhosts"
```

Tempo total passado desde o primeiro pacote trapaceado: < 16 segundos
A conexão trapaçeada agora é fechada: **veja script no cd**

Nós agora vemos RSTs para restaurar as conexões "entreabertas" e esvaziar a fila de conexão para server.login:

veja script na cd

o server.login pode novamente receber conexões.

Depois que o acesso root foi conseguido via trapaça de endereço IP, um módulo do kernel chamado "tap=2.01" foi compilado e instalado no x-terminal:

```
x-terminal% modstat
Id Type Loadaddr Size B-major C-major Sysnum Mod Name
1 Pdrv ff050000 1000 59. tap/tap-2.01 alpha

x-terminal% ls -l /dev/tap
crwxrwxrwx 1 root 37, 59 Dec 25 14:40 /dev/tap
```

Isso parece ser um módulo STREAMS do kernel que pode ser empurrado em uma pilha STREAMS existente e usado para manter o controle de um dispositivo tty. Isso foi usado para conseguir o controle de uma sessão de login já autenticada para o alvo entre as 14:51 PST.

É claro, nenhum ataque pode estar completo sem um toque pessoal. Olhe só:

ftp://ftp.sdsc.edu/pub/security/sounds/tweedle-dee.au
ftp://ftp.sdsc.edu/pub/security/sounds/tweedle-dum.au

Esses estão em formato de arquivo de audio Sun, 8-bit u-law, taxa de amostra de 8 khz.