INVASÃO, SEGURANÇA, TÉCNICA, GESTÃO DE SEGURANÇA E POLÊMICA

proteção

Hacker security

O pior ano da internet

Conheça o dossiê completo do ano da falsificação e tudo mais que o marcou

Hacker que bicho é esse?

Saiba realmente quem é ele! Em primeira mão, o relatório sobre as novas culturas hackers

A falha do CPanel 5

analisada por um

Deface

HaxOrs Lab

O IPV6

O futuro da internet

Por que todo mundo está falando deste protocolo?

Exclusivo! fonte do Mydoom

Os bastidores do worm que derrubou a SCO e ameaçou a Microsoft e a SCO código fonte no CD-Rom

Plano Diretor

Saiba como criar um plano de contingência de segurança

wireless

Sai o WEP entra o WEPA

O fator segurança

Uma galeria de códigos de vírus para seu estudo

EDITORA escala

Ano 01 - nº 07 - R$ 9,90

ISSN 1678-8478

07

9 771678 847006

EDITORA escala

Editora Escala Ltda.
Av. Profª Ida Kolb, 551 - Casa Verde
Cep.: 02518-000 - São Paulo - SP
Tel.: (11) 3966-3166 - Fax.:(11) 3857-9643
Internet: www.escala.com.br
E-mail: escala@escala.com.br
Caixa Postal 16.381
Cep.: 02599-970 - São Paulo – SP

Proteção Hacker

Presidente: Hercílio de Lourenzi
Vice-presidente: Mário Florêncio Cuesta
Diretor Comercial: André Blumberg
Diretor Financeiro: Jack Blumen
Direção Editorial e Marketing: Paulo Afonso de Oliveira
Gerência Editorial: Sandro Aloisio
Supervisão Editorial: Priscilla Mara Ribeiro e Angelo Di Martino
Publicidade e Propaganda: Fernando Fiszbein
Pré-impressão: Douglas Lastri, Eduardo Nojiri, Giliard Andrade, Leandro Siman, Paulo Nery.e Vitório Bettini
Controle de Qualidade/texto: Ciro Mioranza, Maria Nazaré Baracho e Jorge Mazieri
Circulação: Jane Cristina da Silva e Leandra Spinelli
Atendimento ao leitor: (0xx11) 3966-3166 ou atendimento@escala.com.br
Coordenação: Anne Vilar
Atendentes: Adriana Ferreira, Fernanda Alves, Letícia Sbardelotto, Ligia de Campos e Sheila Fidalgo
Conselho Editorial: Amélia Pessôa, André Lima, Carlos Gonçalves, Carlos Mann, César Nemitz, Eddie Van Feu, Fábio Kataoka, Franco de Rosa, José Romeu Feixas, Marcos Evandro, Marques Rebello, Moacir Costa, Moacir Torres, Paulo Fernandes, Paulo Paiva, Pricila Del Claro, Renato Rodrigues, Rick Mann, Robson Oliveira, Rosana Braga, Rosely Ribeiro e Victor Rebelo.
Edições Anteriores: Através do telefone: (0XX11) 3966-3166 ou www.escala.com.br
Impressão e Acabamento: Oceano Ind. Gráfica
Tel.: (011) 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 das edições anteriores da Editora Escala enquanto houver estoque.
Observação Importante
O estúdio *NOME ESTÚDIO* que criou, produziu e realizou este projeto tem inteira responsabilidade sobre a originalidade e autenticidade de seu conteúdo.

Filiada à ANER www.aner.org.br

Criação e Projeto:
MidWest Visual Design

Editor Chefe: Fábio Kataoka
editor@mwg.com.br

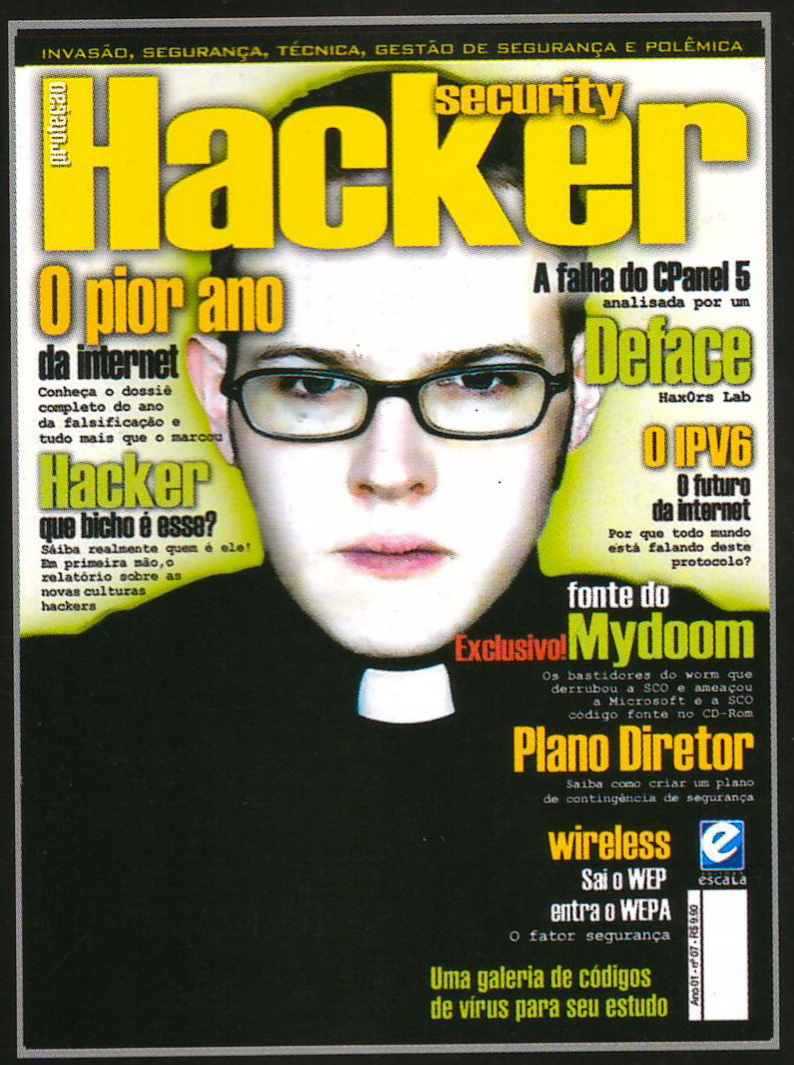
Diretor: Fausto Kataoka

Coordenação Editorial e Direção de Arte:
Marcelo Romano

Reportagem:
Sinval Filho

Executivo de vendas e negócios: Sérgio Ricardo Biagio
Coordenador de trafego: Carlos E. Kataoka
Revisão: Maria Zenólia Almeida
Administração: Agnaldo Torres e Rachel Pereira

Rua Ferreira de Almeida, 73 - SP
Fone: 11 6851-4385
Redação e comercial:
informatica@mwg.com.br



A cada ano a internet se assemelha mais a um campo de batalha. De um lado as grandes corporações desenvolvedoras e provedoras de acesso, de outro usuários tentando desesperadamente se informar e se precaver das deficiências de segurança, dos sistemas, softwares e por fim o "hacker".

Afinal quem são estes "hackers"? Eles parecem sempre estar à frente dos outros. O que as empresas estão fazendo para previnir-se? O que está surgindo de novidade tecnológica?

2003 ficou conhecido como "o ano da falsificação" um verdadeiro caos, Este ano, já surgiu o Mydoom. Mas o que significa esta praga para a internet?

Bem, são estes e outros assuntos que trazemos para você nesta edição. Seja você um segurança ou um hacker.

Colaboradores, participem da próxima edição

A revista Proteção Hacker abre espaço para você, profissional, que deseja participar das próximas edições. Mande um e-mail com os assuntos que deseja ler ou envie um artigo de sua autoria para o endereço:

editorialph@yahoo.com.br

cybercultura

Lançado no Brasil autenticador para redes Nortel

A Secure Computing, empresa de segurança em redes, anunciou o lançamento no Brasil do SafeWord for Nortel Networks, um programa de autenticação para redes virtuais privadas (VPN) da Nortel. O programa tem instalação rápida e pode ser integrado ao Microsoft Active Directory, um serviço que controla permissões em redes corporativas. Segundo o anúncio da empresa, o SafeWord elimina os riscos de segurança causados por senhas fixas que podem ser roubadas, descobertas ou simplesmente perdidas, gerando automaticamente tokens (dispositivos para autenticação) em cada login do usuário.

O SafeWord permite também a auto-inscrição dos tokens, atualização de PINs (números de identificação pessoal) e teste dos autenticadores, simplificando o processo de disponibilização dos dispositivos. Segundo a Secure Computing, isso permite que as empresas economizem até 80% do custo da assinatura e distribuição de tokens. No Brasil, o programa pode ser obtido com as distribuidoras Dedalus, CSC e InteliRedes

Governo federal prepara plano de migração para o software livre

O plano detalhado de migração para o Linux em diversos ministérios foi anunciado em fevereiro de 2004. "Lendo a TI & Governo desta quinzena (newsletter governamental) nos deparamos com a notícia de que o Governo Federal considera o ano de 2004 como fundamental para a implantação de software livre."

Veja uma citação do Sérgio Amadeu (presidente do ITI) do artigo mencionado: "*Nossa idéia é migrar quase plenamente um conjunto de ministérios estratégicos, que permitam demonstrar claramente as vantagens de segurança, compatibilidade, portabilidade e redução de custo do software livre no governo.*"

A TI & Governo é um newsletter semanal em formato PDF, mas como é comercial não consegui descobrir se podiamos ou não colocar o artigo na integra. Nesta edição desta-se mais uma matéria interessante, sobre a criação de um "Linux seguro" (a exemplo do que a NASA fez nos EUA), para uso em algumas aplicações de interesse da segurança nacional. O projeto está a cargo do ITI e do CEPESC, que é um órgão da ABIN, e deve ter uma primeira versão em julho. Assinaturas do TI & Governo 11 3178-1033

Mydoom cresce mais de 3000% no Brasil

Infoguerra

O número de infecções pelo worm chegou a crescer 3.133% em um dia no País. De acordo com as estatísticas do serviço online World Tracking Center (WTC), da Trend Micro, em 27 de janeiro de 2004, o Brasil estava em 7º lugar no Top 10 de países mais infectados.

O Mydoom utiliza truques de engenharia social para enganar o internauta e conseguir se instalar no sistema.

O worm chega por e-mail e os campos de assunto, corpo da mensagem e nome do arquivo anexo, que carrega o código malicioso, variam bastante. Em geral esse vírus chega como se fosse uma mensagem de erro de um servidor para o qual a pessoa teria enviado um e-mail, o que pode provocar a curiosidade do usuário e fazê-lo clicar no anexo, instalando o vírus.

A praga também usa a rede de compartilhamento de arquivos KaZaA para se distribuir. Outro perigo apresentado por ele é a instalação de um cavalo de tróia na máquina contaminada, o que permite o roubo de informações e a manipulação remota do sistema. Além disso, o Mydoom também tenta lançar um ataque DoS (negação de serviço) contra o site da SCO, empresa que trabalha com sistemas Unix e que entrou em choque com distribuições Linux no ano passado.

O Mydoom atinge sistemas rodando Windows 98, ME, NT, 2000 e XP e se dissemina com bastante eficiência. O worm causa lentidão na Internet, congestiona as redes corporativas e, em alguns casos, chega a "derrubá-las".

Os internautas que não estiverem com seu antivírus atualizado podem utilize o serviço **HouseCall** da Trend Micro, ferramenta online e gratuita para verificar e remover vírus.

Microsoft oferece recompensa pelo autor do MyDoom.B

Helena Nacinovic - Infoguerra

Depois da SCO, a Microsoft ofereceu uma recompensa pelo criador do worm MyDoom. A empresa está oferecendo US$ 250 mil para quem fornecer informações que levem à captura do criador do worm W32/MyDoom-B. Este fato dá continuidade ao programa de recompensas da Microsoft, que já ofereceu prêmios semelhantes pela captura dos criadores do Blaster e Sobig.F.

O worm MyDoom.B foi criado, entre outras coisas, para realizar um ataque de negação de serviço (Dos-Denial of Service)contra o site da Microsoft nos EUA, www.microsoft.com. A recompensa oferecida pela Microsoft pelo MyDoom.B também dá seqüência à recompensa de mesmo valor oferecida pelo SCO Group para a captura dos responsáveis pelo MyDoom.A, que foi programado para fazer um ataque de negação de serviço contra o site www.sco.com e já é considerado o worm de disseminação mais rápida da história.

Segundo a Sophos Antivírus, parte do código do MyDoom.B pode conter uma pista para o rastreamento do criador da praga. A linha do código "sync-1.01; andy; I'm just doing my job, nothing personal, sorry" pode conter o nome do autor, mas a suspeita de que o criador do worm teria deixado essas informações como pistas falsas não foi descartada.

A empresa de segurança britânica mi2g afirma que os dois worms da família MyDoom continuam se espalhando com grande velocidade e não mostram sinais de diminuir o ritmo de disseminação. Ambos instalam backdoors, que abrem portas TCP/IP nos computadores infectados, assim esses computadores transformam-se em "zumbis" que estariam sendo exploradas por hackers de vários países, especialmente no Brasil, EUA e Alemanha, segundo a empresa. Os estragos causados pelo MyDoom já chegaram a um ponto que até o FBI está engajado numa investigação global para identificar os autores do vírus.

cybercultura

O Ravel trazendo a luz do conhecimento aos desafios do dia-a-dia

O Ravel (Laboratório de Redes de Alta Velocidade), da Coppe/UFRJ está ligado ao Programa de Engenharia de Sistemas e Computação (PESC/Coppe). Foi inaugurado em 1988 como resultado de um convênio assinado com a 3Com. Os objetivos do Ravel estão em consonância com os da Coppe, envolvendo o desenvolvimento de atividades ligadas à pesquisa, ensino e extensão.

As atividades do Ravel envolvem ainda projetos, modelagens e avaliação de desempenho de redes, desenvolvimento e estudo de diversas aplicações (multimídia, voz sobre IP, gerenciamento, entre outras), além, obviamente, do estudo de todos os aspectos que envolvem a segurança da informação.

Situa-se no bloco I-2000 um moderno complexo de laboratórios do Centro de Tecnologia da UFRJ. Como o Ravel, o I-2000 foi construído através de parcerias envolvendo a Coppe, agências públicas de fomento e a iniciativa privada.

A maioria dos pesquisadores do Ravel é formada por alunos dos cursos de Pós-Graduação da Coppe. Muitos desses alunos iniciaram a sua participação no Ravel ainda jovens, quando cursavam a graduação em Informática ou Engenharia. O laboratório é coordenado pelo Professor Luís Felipe Magalhães de Moraes, idealizador do Ravel e principal incentivador dos estudos que envolvem aspectos de segurança. Particularmente, o Prof. Luís Felipe tem interesse nessa área, tendo desenvolvido pesquisas ligadas à criptografia e teoria da informação desde 1978, época em que fazia o seu curso de doutorado, na Universidade da Califórnia em Los Angeles (UCLA).

No processo de pesquisa exercido dentro do laboratório, o Prof. Luís Felipe é responsável pela canalização do ímpeto jovem dos estudantes, buscando concentrar o conhecimento desses verdadeiros "hackers" com relação a diversos aspectos de segurança, tornando em algo positivo, construtivo e dentro da legalidade. Boa parte das atividades de pesquisa e dos resultados de projetos realizados no Ravel são orientados para uso e aplicações na Rede-Rio de Computadores. A Rede-Rio é uma rede acadêmica e de pesquisa, financiada pela Faperj (Fundação de Amparo a Pesquisa do Estado do Rio de Janeiro) e responsável pelo provimento do acesso à Internet da comunidade de Ciência e Tecnologia no Estado do Rio de Janeiro.

Dessa forma, o Laboratótio Ravel e a Coppe/UFRJ são responsáveis pela coordenação técnica da Rede-Rio, que é exercida pelo Prof. Luís Felipe. Assim sendo, o Ravel colabora também para a disseminação e uso das tecnologias, serviços e aplicações de rede, que são diretamente repassadas e colocadas à disposição dos usuários da Rede-Rio/FAPERJ.

Em 2000, o Ravel lançou na Internet o portal Lockabit, criado em conjunto com profissionais do PESC/Coppe e com apoio da FAPERJ. O Lockabit é a interface entre o conhecimento adquirido pelo laboratório e pela universidade, e o mundo exterior, ou seja, e os profissionais e usuários de segurança.

Na área de segurança o Ravel tem atuado em criptologia (algoritmos de criptografia e criptoanálise), gerenciamento integrado de sistemas de segurança (IDS e Firewall), IPSec/VPNs, PKI, técnicas de segurança para redes sem fio, cálculos de variações de desempenho sob o uso de métodos de segurança e outros temas. Esta é uma área muito abrangente, que pode incluir desde segurança de acesso físico (das pessoas a certos lugares que devem ser protegidos por abrigar sistemas de acesso restrito) até a segurança dos bits que transitam entre máquinas ligadas à Internet.

O Ravel trabalha acreditando que a universidade é o veículo principal para o avanço da ciência e da tecnologia. Quanto mais integração entre as universidades e as empresas, que em última instância, são os usuários da tecnologia, mais conhecimento poderá ser gerado e devidamente aproveitado pelos usuários finais. A tecnologia, na verdade, é desenvolvida através do conhecimento científico e a ciência nasce na universidade.

Fernando Verissimo

Processador com tecnologia ótica em vez de silício

Uma empresa israelense desenvolveu um processador que usa tecnologia ótica em vez de silício, o fato que permite a realização de operações de computação na velocidade da luz. A empresa, chamada Lenslet, diz que seu processador poderá ser usado em aplicações militares e de segurança nacional, multimídia e telecomunicações.

"O processamento ótico é uma vantagem competitiva e estratégica para nações e empresas", disse Avner Halperin, vice-presidente de desenvolvimento comercial da empresa. "Processando na velocidade da luz, você pode ter aeroportos mais seguros, sistemas militares autônomos, sistemas de transmissão de multimídia em alta definição e avançados equipamentos de próxima geração para telecomunicações."

O novo processador foi desenvolvido para equipar radares de alta resolução, sistemas de guerra eletrônica, estações-base de telefonia celular e aparelhos de exame de bagagens em aeroportos. A Lenslet afirma que o dispositivo, chamado Enlight, é o primeiro DSP ótico disponível comercialmente. Ele foi apresentado na conferência MILCOM, em Boston, nos EUA, no início desse ano.

Microsoft quer limpar sua imagem

Melhorar a segurança. Esta é a palavra de ordem na organização de Bill Gates. Provadisso é o novo grupo criado pela Microsoft, que, entre outras funções, vai dedicar-se à criação de novos processos de desenvolvimento, de novas ferramentas para os programadores desenvolverem programas mais seguros.

A principal missão da Security Engineering Strategy (SES) vai ser a análise dos índices de segurança de todos os produtos da multinacional De Redmond, de forma a melhorar a qualidade das soluções. De acordo com Steve Lipner, diretor do recém-criado grupo, a nova divisão pretende transmitir aos clientes a idéia de que a segurança é uma das prioridades da multinacional, ajudando assim a limpar a imagem de que os produtos da Microsoft têm muitas falhas.

O líder da nova divisão revelou que a segurança de muitos dos produtos da Microsoft devem ser revistas e melhoradas. Este grupo, de acordo com o fabricante, tem uma equipe especializada cuja principal função é descobrir as falhas dos produtos internamente, antes que sejam descobertas por alguém fora da empresa, o que permite preencher as lacunas antes que estas provoquem estragos.

À medida que as falhas são eliminadas, a Microsoft consegue melhorar os seus processos e passa a desenhar um código cada vez mais seguro.

Hacker adolescente se faz passar por ministro da educação

Um jovem de 15 anos, natural de Singapura, se passou pelo ministro da Educação do seu país por meio da da Internet, segundo informação de um jornal local.

O adolescente pediu a expulsão de dois dos seus colegas de turma por meio de um comunicado, que tudo indicava provir do Ministério da Educação. De acordo com o menor, ele não gostava de um dos alunos devido a uma briga. O outro nome foi só para disfarçar a situação.

O erro do jovem foi reenviar o e-mail ao ministro que, desde logo, alertou o colégio. O juiz, que declarou que o adolescente era um "obcecado pelo poder" e que devia aprender a ter relações sociais, o colocou sob vigilância durante dois anos e o condenou a 240 horas de trabalho comunitário.

"o ano da falsificação"

2003: O pior ano na história da Internet

Hubiratan Neto | udneto@yahoo.com.br

O ano de 2003 para alguns foi considerado como "o ano da falsificação". Para outros, como "o ano do Spam" e para os mais alarmistas, o ano em que "o DDOS poderia vir a se tornar o câncer da Internet".

Felizmente, sobrevivemos a tudo e a todos (como sempre), e cá estamos, dispostos a prever o que o destino nos prepara para 2004.

Mas e se eu lhe perguntasse quais foram os 20 acontecimentos mais marcantes de 2003 na área da segurança da informação?

Assim fica difícil, eu sei... E foi pensando nisso que nós, da Proteção Hacker, preparamos uma retrospectiva inédita, ou seja, uma revisão dos acontecimentos mais marcantes deste ano tão repleto de Falsificações e Spams, uma retrospectiva para ser guardada a sete chaves como relíquia, afinal de contas, e antes de mais nada, 2003 foi o ano da Segurança da Informação.

JANEIRO

Mitnick de Volta à Web

O mundo aguardava ansiosamente a chegada do dia 21 de janeiro, pois após oito anos longe dos modems e já com 39 anos de idade, o "hacker" Kevin Mitnick (www.kevinmitnick.com), um bauzaquiano que já foi o hacker mais procurado pelo FBI por invadir sistemas de empresas como Sun, Motorola, Nokia e Novell, se conectaria à Internet novamente.

"Meus amigos e minha família estão cansados de checar as mensagens para mim", desabafou: "Não posso mudar o passado, mas já paguei minha dívida com a sociedade e estou tentando fazer uma coisa positiva."

Pkasa oferece emprego de 5000 dólares... Interessado?

Depois de enfrentarmos o Klez em 2002, tivemos de lutar contra o Pkasa, o primeiro vírus de 2003 na internet.

Nem o KaZaA escapou de se tornar um disseminador do vírus, que entre outros meios, contaminava suas vítimas via e-mails, drivers, redes locais e canais de bate-papo.

O Pkasa tinha como principal finalidade desativar os programas de segurança dos computadores contaminados, tais como antivírus e firewalls. Possuía como principal atrativo quando recebido via e-mail, o seguinte subject: "trabalho em casa para ganhar 5000 dólares por mês".

Um verdadeiro terror para os "clicadores compulsivos".

Enquanto uns sobem, outros caem...

Neste mesmo mês, a Microsoft Corp. anunciou ao mundo seu lucro líquido obtido durante o ano de 2002 as cifras chegam a US$ 2,55 bilhões. Já a Sun Microsystems, não fazia tanta questão quanto a Microsoft de anunciar seus números, que foram de US$ 2,28 bilhões, só que NEGATIVOS! 2002 foi considerado pela empresa Sun como o ano em que a companhia somou o maior prejuízo líquido de sua história, depois de assumir encargos de mais de 2 bilhões de dólares causados principalmente por perdas em investimentos.

Vírus, Exploits, Trojan e Spam, muito Spam!

Em 2003 foi também o ano em que o Spam deixou de ser novidade para se consolidar como uma das pragas do mundo da Informática ao lado dos vírus e trojans.

Neste mesmo ano todos os antivírus já passariam a trazer consigo módulos próprios para o controle de e-mails indesejados. Este controle também passou a ser realizado por quase todos os Webmails públicos do mundo.

"Windows ganha mais uma do Pingüim!"

Durante todo o mês de janeiro, o Zone-H divulgou sua lista mensal de invasões e relatou que 53% das invasões bem-sucedidas a sistemas eram direcionadas ao MS Windows contra 34% do Linux.

FEVEREIRO

Procura-se vivo ou morto, de preferência, online...

Fevereiro literalmente não foi um bom mês, pelo menos para o Cracker Guilherme Amorim de Oliveira Alves, 18 anos, que foi preso pela Polícia Federal no dia 20, em Petrópolis (região serrana do Rio de janeiro), por clonar sites de instituições bancárias do Brasil e do exterior e aplicar golpes em correntistas pela internet. Entre os Bancos clonados estavam o Bradesco, a Caixa Econômica Federal e o Banco do Brasil, além de bancos Internacionais.

Além dos Bancos citados, o Cracker já havia sido preso em 2002 por possuir dados de cartões de créditos de 3,5 mil clientes das instituições Mastercard e American Express.

Como por trás de um grande homem há sempre uma grande mulher, a namorada do cracker, Maria Cecília Faria Martins, que mora em Americana, São Paulo, também foi presa por participação ativa em todos os atos de seu amado cracker.

Procura-se vivo ou morto, de preferência, online. - Parte II

Parece que foi combinado, mas por incrível que pareça não. No mesmo dia em que a policia prendia o cracker Guilherme Amorim de Oliveira Alves, Ricardo Braz Damasco também foi preso no Rio de Janeiro, acusado de fazer compras em lojas virtuais tais como Lojas Americanas e Ponto Frio com números de cartão de crédito de outras pessoas. Coincidência ou não, e, por via das dúvidas, foi todo mundo pro xadrez!

MARÇO

Cyberlords Vs. George Bush

Ainda neste mês o grupo Cracker brasileiro Cyberlords invadia uma série de sites cubanos para protestar de maneira "pacífica" contra a Gue..... Bem, não precisa dizer mais nada, o resto todos podem imaginar.

O cracker que vai pro céu!

Adrian Lamo, um homem de bem (vai nessa...) informava amigavelmente ao Blogger.com sobre um furo de segurança que permitia que qualquer blog fosse facilmente alterado.

A Pyra , empresa responsável pelo serviço agradeceu publicamente ao cracker "bonzinho" dizendo: "Adrian Lamo é um hacker do Bem". cracker do bem?? Fala sério!! No mínimo o cara queria um emprego e se deu mal... Esse golpe é igual ao do baú...bem conhecido e divulgado!

Até o site do jornal iraquiano Al-Jazeera foi bombardeado...

Nem Alá conseguiu parar os ataques ao site Al-Jazeera durante o mês de março. O mesmo, quando ficava on-line por alguns minutos, era novamente invadido e, para variar, pichado. As pichações, todas partidas de grupos crackers Norte-americanos diziam palavras do tipo "deixem a liberdade acontecer" ou "Deus abençoe nossas tropas". Por Alá, alguém se habilite a criar um Firewall para o Al-Jazeera!

Gigantes da computação criam grupo anti cracker

Criado o Trusted Computing Group - TCG, a partir da união de grandes empresas de tecnologia como AMD, HP, IBM, Intel, Microsoft, Philips, Nokia, Atmel, Infineon, ST Microelectronics, Phoenix Technologies, National Semiconductor, Sony, Wave Systems e VeriSign. A idéia é desenvolver padrões abertos de segurança direcionados a produtos e serviços de tecnologia e computação para todos os tipos de aparelhos (de PC´s a celulares)

Quer uma opinião pessoal? Se a Microsoft faz parte do grupo é sinal de que o projeto provavelmente vai "travar" ou "dar pau".

ABRIL

A Microsoft pode ser segura?

Pesquisa realizada pela Forrester Research neste mês demonstra que 74% dos Gerentes de TI não confiam na segurança dos produtos da Microsoft Corp.

A pesquisa foi realizada com gerentes de 35 empresas cujo faturamento é maior do que um bilhão de dólares anuais. Além dos problemas na segurança, os gerentes complementaram: "é muito trabalhoso administar a plataforma." Irônico, não?

Morte aos Spammers!

O Spammer profissional George A. Moore Jr foi literalmente caçado por milhares de pessoas. Adivinhe por quê?

Francis Uy, maior inimigo do sr. George Moore, fez questão de divulgar em seu site anti-spam (http://spamreaper.com/frankie/spam.html) os endereços e telefones dos spammers de plantão para que os mesmos fossem contatados pessoalmente por suas "vítimas" e, é claro, para que pudessem ir aos mesmos pessoalmente e dizer: "Pelo amor de Deus, nos deixe em paz!" O sr. Moore, um dos maiores spammers da internet, teve sua vida completamente invadida e recebeu (segundo o mesmo) mais de 800 telefonemas entre xingamentos, ameaças de agressão e até mesmo de morte.

Cracker pode ser condenado a passar o resto da vida na cadeia

O cracker texano Jason Jarrell de 19 anos pode ser condenado a passar 95 anos na cadeia sob a acusação de invadir os sistemas da Universidade de Yale, Texas - EUA. As invasões ocorreram ainda no ano 2000, quando o cracker tinha apenas 16 anos.

Jarrell, segundo os dados incorporados ao processo, instalou Spy´s e Backdoors na Faculdade de Yale, Bass Laboratory e do Wright Nuclear Structure Laboratory, causando então um prejuízo calculado em 150 mil dólares. A pergunta agora é: "Será que Jason Jarrell será o Kevin Mitnick do segundo milénio?" Se for, vamos mais à frente...Free Jason!!

MAIO

Trinity usa Linux para invadir a Matrix...

Finalmente, em 23 de Maio de 2003, saiu do forno o tão esperado "The Matrix Reloaded"

O filme, regado a muita ação e filosofia, nos trouxe algumas revelações interessantes. Acreditem, Trinity faz parte da comunidade GNU/Linux. Para os que não acreditam, reparem que a mesma, ao invadir o sistema da matrix em uma das cenas do filme, utiliza o Nmap e um Exploit de ssh (todos softwares reais). Infelizmente só não se pode afirmar que a Matrix roda Windows, pois o Nmap não conseguiu detectar o sistema da vítima. O fato é que esta é a primeira vez que um filme sobre o tema "Hackers que lutam Kung-Fu" utiliza softwares reais de invasão para compor os roteiros. Mais uma vez, palmas para os irmãos Wachowski.

Pra variar, mais um bug no Windows 2000

Crackers conseguiram, via ataque DOS (Denial of Service) executar programas remotamente em sistemas Windows 2000, explorando então falhas do Windows Media Services(WMS) que nada mais são do que funções que dão suporte à distribuição de conteúdo de mídia por meio de um sistema chamado multicast streaming.

A Microsoft, como é de costume, disponibilizou a correção do bug logo que o mesmo foi relatado.

Deu pau na SCO

O sr. Darl McBride, um dos maiores executivos da SCO, ameaçou processar Linus Turvalds por utilizar-se das bibliotecas de seu sistema para compor o Sistema Linux.

Este foi o primeiro episódio da comédia "SCO Vs. O Mundo". E isso não foi tudo, logo após a declaração do sr. McBride, a SCO ainda chegaria ao ponto de ameaçar todos os usuários do sistema Linux de processo judicial.

A resposta da comunidade GNU e de Linus Turvalds? Nenhuma... Afinal de contas, quem não deve, não teme!

Servidores Linux sofrem 19 mil invasões em apenas um mês

Divulgada pelo Zone-H a lista de invasões do mês de Maio, segundo a mesma, o Linux obteve 19.208 invasões apenas neste mês.

O número foi atribuído ao crescimento do Linux em servidores Web, e-mail e firewall. Mesmo assim, Windows e Linux continuam lado a lado nesta guerra onde ter menos vale mais...

invasão

RETROSPECTIVA

JUNHO

Clonaram um BB

Calma, ainda não foi desta vez que uma criança foi clonada, o BB mencionado trata-se na verdade do Banco do Brasil. O site da instituição foi clonado com o intuito de roubar dados dos clientes, como números de contas, senhas etc.

Para cair na armadilha dos crackers os clientes precisavam receber um e-mail que continha um anúncio de que o mesmo poderia vir a ganhar um prêmio em dinheiro do banco. Para isso, bastava clicar no link indicado no próprio e ir parar direto ao site clonado. Lá, o cliente... quer dizer, a vítima, digitaria sua agência, conta e senha... Fácil, não?

Apenas como esclarecimento e segundo nota oficial do próprio Banco do Brasil, o mesmo não envia e-mails aos seus clientes, exceto quando é expressamente autorizado por eles, somente para a remessa de boletins e informativos. Quanto aos procedimentos de troca de senha, só podem ser efetuados no próprio site do Banco, nos terminais de auto-atendimento ou nas agências.

Veja o e-mail que deu muita dor de cabeça aos clientes do bb.com.br, e o que não deixa de ser um ótimo exemplo de engenharia social:

A forte e consistente política de investimentos em tecnologia (R$ 2,1 bilhões investidos nos últimos cinco anos) tem permitido ao Banco do Brasil a constante melhoria na qualidade de seus produtos e serviços o Banco do Brasil agora está oferecendo aos seus clientes o BB E-Mail Banking de acesso gratuito. Que facilita você realizar suas movimentações bancárias mas seguras através do Internet E-mail Banking com total segurança e com certificado digital que lhe dá a total confiança nas suas transações bancárias.*

Tenha total segurança durante suas movimentações bancárias. Você acessa a internet todos os dias para ler seus e-mails. Logo, seria prático e inteligente receber informações da sua conta , como saldos, extratos e lançamentos também por e-mail. Já imaginou você poder efetuar um resgate, aplicação ou pagamento de contas por meio de um atalho e mais: informações e dicas exclusivas de investimento, além dos principais índices financeiros, cotações, fundos e ações.

Clientes que cadastrarem no BB Internet E-Mail Banking até o dia 30 de junho podem ganhar prêmios e sorteios mensais de R$ 50 MIL.

O cracker astronauta

É de conhecimento público que não existe nada mais fácil do que invadir o sistema de uma universidade, dito que geralmente o Sysop da mesma é algum professor de ciência da computação ou análise de sistemas que se acha extremamente genial e expert em tudo... Digamos que é como tirar doce de criança.

Como dificilmente acharemos uma exceção a esta regra, o The Japan Times (não precisa nem dizer que se trata de um jornal do Japão :) publicou em junho de 2003 a notícia de que a universidade de Kobe recebeu e-mails da NASA perguntando mais ou menos o seguinte: "*ei, o que vocês querem em nossos servidores?*"

Surpresos, os responsáveis pela mesma resolveram investigar e descobriram que um cracker havia invadido seus sistemas e instalado Spy´s e Softwares que realizavam varreduras em outras redes, entre elas a da Nasa.

A medida de segurança adotada pela Universidade? Retirar o servidor da rede... é mole?

Que eles são bons de Karatê não se discute, mas de segurança de sistemas...

Microsoft não sabe fazer Antivírus

A Microsoft, como parte da iniciativa Trustworthy Computing, fechou um acordo com a GeCAD, empresa romena de antivírus, que permite a integração de seus produtos com os softwares da mesma. A pergunta agora é: Por que a própria MS não fabrica seu antivírus?

Dizem as más línguas que se a mesma embutisse antivírus ao sistema, este não deixaria jamais o Windows ser instalado em um computador...

Mais informações em http://www.ravantivirus.com/pages/shownews.php?i=153

JULHO

O dia em que a Internet parou!

O site defacers-challenge, www.defacers-challenge.com, resolveu promover o evento do ano: "Aquele ou aquela que conseguisse pichar 6000 sites em um menor tempo ganharia a copa do mundo de cracker e seria o melhor". Bem, levando em consideração que o próprio site defacers-challenge foi tirado do ar, o concurso foi um sucesso. Pena que nenhum site pôde documentar o episódio, pois todos foram pichados. Resultado final: ninguém ganhou o concurso de Miss Cracker 2003!

Você se lembra do W32.Bugbear?

E como esquecer do vírus de maior sucesso do ano... o campeão de ibope e que virou matéria do Fantástico!

O worm de propagação em massa arrasou tudo o que encontrou pela frente, ou quem possuía sistemas como Windows 95, 98, NT, 2000, XP, Me instalados em seus computadores e servidores. O worm, que explorava uma vulnerabilidade da família Windows, conhecida como "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment", quando executado, criava uma cópia de si mesmo para o diretório \Iniciar, com isso era executado nas inicializações do sistema, além de enviar e-mails desenfreados a todos os contatos de sua lista de e-mails. Mas para aqueles que se depararam com um *"I Love You"* em sua caixa de entrada, o Bugbear não passou de um grande susto...Ainda bem!

Quem diria, no Casaquistão também existem crackers

O cracker do Casaquistão Oleg Zezev, 29 anos(eu não tenho a menor idéia de como se fala isso) foi condenado a passar quase 5 anos no xadrez por ter invadido o site da Bloomberg.

A história chega a ser curiosa, pois o cracker invadiu os sistemas da Bloomberg e chantageou o seu presidente, sr. Michael Blommberg, afirmando que se o mesmo não pagasse 200 mil dólares, veria as informações confidenciais da empresa divulgadas na Internet e na mídia...

Oleg Zezev, diretor de tecnologia de uma grande CIA casaquistanesa, foi condenado por tentativa de extorsão, conspiração, invasão de computadores e envio de ameaças por e-mail e além disso, terá que pagar indenização de 950 mil dólares ao sr. Bloomberg. É amigos, literalmente, o crime não compensa!

Ei, também tem Cracker na Romênia!

Crackers Romenos ameaçaram empresas norte-americanas e pediram resgates que chegaram a 50 mil dólares por informações confidenciais das mesmas.

O FBI, que adora casos que envolvem cyberterroristas (que é como costuma denominar os crackers) prendeu todo mundo e publicou que todos os romenos não possuíam nem ao menos o segundo grau completo, além de estarem todos desempregados. A prisão não durou mais do que 30 dias. Lá na terra do Tio Sam, pelo jeito, as coisas também acabam em pizza!

AGOSTO

Cracker deita e rola durante dois meses no gnu.org

Nem o repositório de softwares da Free Software Foundation (http://ftp.gnu.org/) escapou dos crackers no ano de 2003. O site foi invadido ainda no mês de março, o que deu todo o direito do cracker deitar e rolar nos arquivos disponíveis para download no site.

O invasor, que conseguiu privilégios de root, teria alterado alguns programas e os disponibilizado para download, além de instalar trojans nos servidores da FSF.

Para os desavisados, a FSF publicou a lista dos softwares que possivelmente foram alterados pelo cracker. A relação pode ser encontrada em http://ftp.gnu.org/MISSING-FILES.

WindowsUpdate na mira!

Em agosto foi a vez do virus Blaster torrar a paciência do sr. Gates III.

O vírus, por incrível que pareça, iria comandar um ataque DDOS (Negação de serviços em massa) ao site WindowsUpdate.com no dia 17 de agosto.

A Microsoft, é claro reforçou o firewall... que nada, ela apenas tirou o site do ar. Quer medida de segurança melhor? Vírus? Desplugue o cabo da rede e pronto!

Este é um pequeno exemplo das inovadoras soluções de Security da Microsoft Corp...

Open-Source "DDOS" na SCO

Ainda sobre a novela "SCO Vs. O Mundo", um certo cracker, simpatizante da comunidade GNU, e pelo jeito bastante irritado com as declarações e agressões da SCO ao Linux, procurou resolver o problema. A Solução? Comandar um ataque DDOS ao Site da "Amiga" SCO. A SCO, bastante magoada com o ocorrido, declarou que o ataque causou prejuízos a seus negócios e que não mediria esforços para descobrir a origem real dos ataques. Já Eric Raymond, presidente da Open Source Initiative, desaprovou a iniciativa do cracker GNU declarando: "Nós somos pessoas boas. Não podemos usar o vandalismo, a infração e a opressão à palavra em nossa luta, porque senão a SCO vai nos chamar de crackers e poderá ter razão". Sabe o que o meu lado Sérgio acha desta briga entre a GNU e a SCO? Comprar um computador, R$ 1800,00. Conectá-lo à Internet, R$ 15,00. Ver o site da SCO fora do ar, não tem preço!

SETEMBRO

Todo mundo entrou na dança...

Relatados no mês de setembro vulnerabilidades que comprometiam os softwares e protocolos da Microsoft Corp, Entre eles NetBIOS, Word, WordPerfect Converter, Visual Basic for Applications e Access. Ô mêsinho infeliz para os amigos da M$ Corp!

Executivo perde o emprego por criticar Microsoft

O Sr. Daniel R. Geer, ex-executivo na área de segurança da informação da AtStake foi demitido após participar de um estudo sobre as condições atuais de segurança de computadores e relatar sua opinião pessoal: que o domínio da Microsoft em software torna mais fácil para hackers atacar de uma só vez milhões de máquinas e redes.

O relatório foi barrado também em várias revistas e publicações especializadas, pois, como falar mal de um anunciante tão bom?

O sr. Daniel R Geer não quis comentar o assunto, mas segundo o jornal *The Washington Post,* a ex-empresa do mesmo declarou em nota oficial que "*Os valores e opiniões do relatório não estão alinhados à visão da AtStake*"

Três brechas de uma só vez!

A Microsoft alertou seus usuários no dia 10 do mês de setembro sobre uma falha no protocolo Remote Procedure Call (RPC) de seus sistemas NT 4.0, Windows 2000, XP e Server 2003, que abria três portas para acessos indevidos.

OUTUBRO

Cracker executivo conspira contra o governo norte-americano

Militares dos Estados Unidos foram à caça do empresário da ForesincTec Solutions, pois, segundo os mesmos o sr. Brett E. O´Keefe, 36 anos, invadiu instituições como Exército, Marinha, Nasa e demais órgãos governamentais norte-americanos. Segundo os militares e o FBI, o sr. Keefe tinha como intuito único obter informações confidenciais e, com isso, literalmente "ganhar dinheiro".

Keefe responde a seis processos incluindo o de "conspiração contra o governo". E para variar, declarou que é inocente e que acredita em Papai Noel.

ajudinha!!

NOVEMBRO

Estudante de Economia faz pós-graduação em crackerismo

Van Dinh, 19 anos, estudante de Economia da faculdade de Drexel, Pensilvânia, é preso por realizar golpe on-line a um megainvestidor da bolsa.

O golpe de Dinh foi citado pelo Securities and Exchange Com–mission (a Comissão de Valores Mobiliários americana) como "*um dos golpes via web mais complexos já vistos*"

Com o dinheiro da vítima o garoto conseguiu comprar nada mais nada menos do que 7 200 ações da empresa Cisco, entre outras empresas.

Cansada, usuária processa Microsoft

Usuária norte-americana do Windows processa a MS simplesmente por produzir produtos extremamente falhos.

Segundo dados do próprio processo, a acusação alega que: "a grande maioria dos ataques bem-sucedidos na internet é atribuída a vulnerabilidades sérias no software da Microsoft"

A Microsoft declarou em sua defesa que as acusações de tal usuária "não fazem sentido" até porque "a culpa por estes atos criminosos é de quem cria os vírus", e não da Microsoft que cria sistemas falhos. Culpados ou não, bem que a MS dá uma bela

Linus Torvalds e Richard Stallman são intimados pela SCO

Voltando ao velho assunto "SCO Vs. O Mundo" (que aliás já está ficando cansativo). Foram intimados pela corte de Utah Linus Turvalds: criador do Linux, Richard Stallman, Criador do movimento free software e ainda funcionários e colaboradores da Transmeta, da Open Source Development Lab, da Novell e da Digeo, que produz set-top boxes baseados no OS Linux. Além disso, uma semana antes a SCO enviou a empresas colaboradoras da IBM, que também havia processado a Big Blue.

Office 2003 mal saiu do forno e já tem bugs!

Uma falha causada pela biblioteca Mso.dll transformou a estréia do Office 2003 em uma grande furada...

A Microsoft correu para corrigir o bug mais já era tarde, e, embora o mesmo não seja considerado um furo de segurança, serve para nos dar uma prévia do que vem por ai...

Brasil, o país do futebol, do carnaval e da Internet

Em novembro de 2003 chegamos ao número de 17,2 milhões de internautas no país. Isso quer dizer que 10% de toda a população está conectada à Internet.

Hoje, o mundo possui 825 milhões de pessoas conectadas à Internet, 187 milhões norte--americanos contra 44 milhões da América Latina.

DEZEMBRO

Bug do Kernel 2.4.23 compromete o Projeto Debian

Pelo menos 4 servidores do Projeto Debian foram invadidos durante o mês de dezembro deste, entre eles o que continha os códigos fontes dos sistemas e softwares em desenvolvimento. Segundo os coordenadores do Projeto Debian, o invasor instalou trojans nos mesmos possibilitando que lhe fossem reveladas senhas de usuários reais o com isso acabaria conseguindo facilmente acesso de root aos sistemas.

No momento a Debian se concentra em analisar todos os códigos-fontes dos servidores a fim de garantir total integridade aos mesmos.

Liu Die Yu demonstra 7 falhas no Internet Explorer

Este é o nome do rapaz, Liu Die Yu, o chinês que se tornou o inimigo número 1 do mês da Microsoft Corp.

O cara liberou sem comunicar oficialmente à Microsoft 7 vulnerabilidades que comprometiam totalmente o Navegador Internet Explorer. entre as mesmas, pelo menos duas foram taxadas como altamente críticas.

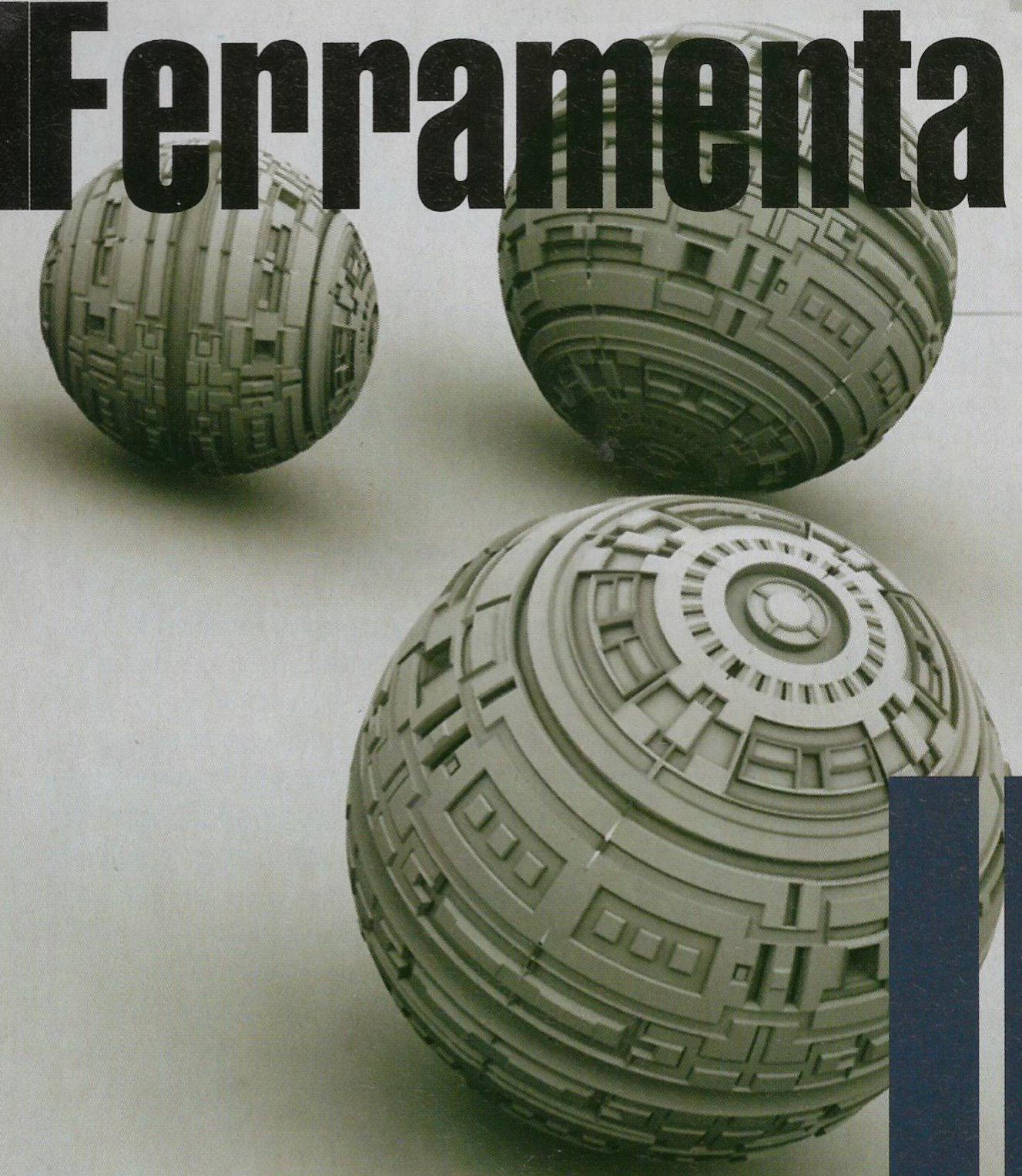
Quem quiser saber mais sobre as falhas relatadas pelo Sr. Liu basta acessar o Site TheInquirer.net.

Bug do Kernel 2.4.23 faz mais duas vítimas

Free Software Foundation e Gentoo também entraram na lista de sistemas comprometidos pelo bug do Kernel 2.4.23, segundo anúncio da Savannah e da própria Gentoo. A pergunta agora é: quem será o próximo?

Informações em http://savannah.gnu.org/statement.html e http://www.gentoo.org/

IPV6



6Bone, IR6 Forum, Kame, ARIN, LACNIC, LATFV6 e BRBONE. Mas afinal, por que todo mundo está falando nesse tal IPV6?

IPV6

Você está preparado?

Hurubatan Neto | udneto@yahoo.com.br

Depois de Vint Cerf e Robert Kahn em 1974, terem criado o TCP-Transmission Control Protocol, chegou em 1978 o IP-Internet Protocol, sob o rítimo de embalos à noite. Unidos viriam a se tornar em 1981 o protocolo padrão da Internet mundial e hoje o mais utilizado do mundo, o TCP/IP.

Apresentava-se ali o berço da Internet que hoje conhecemos tão bem e que após o desenvolvimento do HTTP - Hypertext Transmission Protocol desenvolvido em 1990 por Tim Berners-Lee, um brilhante físico do CERN.

Em sua versão 4, também conhecida por IPV4, o Internet Protocol (IP) possui tudo o que precisávamos para concebermos a maior rede de computadores do mundo, a Internet, pois seu endereçamento de 32 Bits nos permitiria a criação de aproximadamente 4,3 bilhões de endereços de hosts interligados, sem falar que o conceito de uma rede descentralizada seria inteiramente possível, graças a seu modelo de roteamento dinâmico.

Mas tudo bem..., o protocolo é perfeito (ou quase). Sim eu sei, algumas aplicações baseadas em endereçamento IP de origem e destino passaram (e ainda passam) por um bom aperto com o desenvolvimento de técnicas de Spoofing (que o diga nosso velho amigo Shimomura!), mas isso era um detalhe que poderia ser minimizado com um pouco de criptografia.

Foi então que o protocolo criado por Berners Lee tornou-se a ponta do Iceberg, ou seja, sendo a Internet tão acessada pelo público em geral (e porque não dizer consumidores em potencial) e interessante o bastante para aplicações de cunho comerciais e empresarias, 4,3 bilhões de endereços disponíveis já não eram mas suficientes para conter a mortal e temida "febre da Web".

A "febre da Web" passou então a ser a maior ameaça para aquele protocolo concebido durante os "embalos de sábado à noite". A questão então passou a ser: e se um dia cada um dos 4,3 bilhões de endereços possíveis para o IP versão 4 (IPV4) possuírem donos? E se os IP´s acabarem? O que será do mundo? Como novos computadores poderão se juntar aos demais da rede mundial?

Sabe amigos isso sim seria um grande problema... Já pensou você querendo entrar na internet e tendo que pedir ao seu vizinho um IP emprestado?

E foi pensando nisso que em 25 de julho de 1994, na 25th IETF meeting, realizada em Toronto, EUA, deu-se inicio a uma total reformulação do protocolo IPV4, nomeando-o então de IPV6, ou simplesmente "Internet Protocol versão 6".

Em sua versão 6, o IP acabaria de vez com o medo da escassez de seu endereçamento tal como também significava a promessa de uma Internet mais veloz e segura.

Algumas das interessantes promessas para o IPV6 foram:

- Endereçamento de 128 Bits
- Auto configuração
- Conexão End-to-End
- Criptografia nativa
- Múltiplos endereços por interface de rede
- Sem Broadcast
- Datagrama Melhorado
- Simplificação de Cabeçalho
- Sem máscara de su-redes
- Sem NAT
- Entre Outros...

Tais promessas nos possibilitariam entre outras formais melhorias um aumento considerável de 4,3 bilhões de endereços de hosts (possíveis para o Ipv4) para 340.282.366.920.938.463.463.374.607.431.768.211.456 de endereços de hosts possíveis (para o IPV6), sem falar que um cabeçalho enxuto significa ganho de velocidade e performance tal como criptografia nativa é sinônimo de segurança (até que algum cracker prove o contrário e é claro, dependendo do algoritmo utilizado!).

Enfim, ninguém tem dúvidas de que o IPV6 está preparado para a terrível missão de ampliar os horizontes da Internet... Mas e você, está preparado para o IPV6?

Você pode não ter conhecimento disso, mas todos os grandes fabricantes de softwares do mundo já prepararam seus sistemas para o IPV6 e até o Windows está pronto para ele (quer dizer... afirmar que o Windows está totalmente pronto para alguma coisa é ir contra a própria história do sistema!).

De qualquer forma, um dos maiores problemas enfrentados por países como os Estados Unidos para a implementação do IPV6 é justamente a falta de mão-de- obra especializada. Já países como Suécia e Japão estão financiando com altas contribuições financeiras pesquisas para a implementação bem-sucedida do IPV6.

No Brasil, terra do futebol, do samba e da mulher bonita, tal implementação ainda está sendo estudada pelo BR6BONE, mas o fato é que mais cedo ou mais tarde o IPV6 se tornará o padrão mundial das redes de computadores.

Então vá logo se preparando para os futuros desafios que irá encontrar pela frente... Pois este técnico em segurança de sistemas que vos fala já está correndo atrás do prejuízo.

Ferramenta

WINDOWS

Para os amigos entusiastas do sistema GNU/Linux, aí vai uma preciosa receita de bolo criada por Marcel R. Faria (marcel@rnp.br) para preparar seu sistema do Pingüim para "o tal IPV6".

1 Comece baixando o código-fonte de seu sistema Linux, digamos que ele seja o 2.4.9 você deve ir em http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.9.tar.gz

2 Descompacte-o

```
# tar xvzf linux-2.4.9.tar.gz
# mv linux/ /usr/src/linux-2.4.9
# cd /usr/src/
# ln –s linux-2.4.9 linux
```

3 Configure-o

```
# cd /usr/src/linux
# make menuconfig

Code maturity leve options —>
  [*] Prompt for development and/or incomplete code/drivers
  Networking options —>

  <*> Packet socket

  [*] Kernel/User netlink socket
  [*] Routing messages
  [*] IP: advanced router
  [*]   IP: equal cost multipath (NEW)
  [*]   IP: use TOS value as routing key (NEW)
  [*]   IP: verbose route monitoring key (NEW)
  [*]   IP: large routing tables (NEW)
  <*> IP: tunneling
  <*> IP: GRE tunnels over IP

  <*> The IPv6 protocol (EXPERIMENTAL)
```

4 Modifique a tag EXTRA VERSION para criar uma subversão (opcional)

```
# vi Makefile

EXTRA VERSION = -IPv6
```

5 Compile o Kernel

```
# make dep; make clean; make bzImage; make modules
```

6 Instale os módulos

```
# make modules_install
```

7 Instale o novo kernel

```
# cp /usr/src/linux/arch/i386/boot/bzimage /boot/vmlinuz-2.4.9-IPv6
# vi /etc/lilo.conf

default=linux-ipv6

image=/boot/vmlinuz-2.4.9-IPv6
label=linux-ipv6
read-only
root=/dev/hda1

# lilo –v
```

8 Reboot a máquina

Urubatan D´Oliveira Neto

Especialista em Segurança de Sistemas Gnu/Linux
neto@studiovirtual.com.br

Rastreabilidade:

Controlando o Fluxo das Informações

André Palma, consultor da Axur Information Security | http://www.axur.com.br

A maioria dos profissionais de segurança da informação conceitua a segurança através de três aspectos básicos: confidencialidade integridade e disponibilidade. Isto ocorre devido à grande influência de frameworks e metodologias internacionalmente consolidadas. Entretanto existe um conceito primário associado à segurança da informação que não está sendo adequadamente focado no cenário nacional – a rastreabilidade.

O conceito de rastreabilidade está diretamente relacionado ao controle sobre o fluxo da informação. É necessário identificar de forma ágil e simples como determinada informação se relaciona com o negócio. As perguntas parecem óbvias, mas nem sempre são respondidas. Qual a origem desta informação e para onde esta informação vai? Quais os links existentes entre as informações.?

A discussão sobre esse tema entre os profissionais de segurança da informação não é mera casualidade. O que tem acontecido é que a prática de proteção das informações tem sido sensivelmente prejudicada pela dificuldade de identificação das informações e seus relacionamentos. Garantir a segurança das informações sem identificar claramente seu fluxo é uma tarefa praticamente impossível. A solução pode parecer simples – identificar este fluxo. Porém as informações nem sempre seguem fluxos bem definidos, nem sempre são facilmente rastreáveis.

O mapeamento de processos de negócio muitas vezes se confunde com o mapeamento do próprio fluxo da informação, isto ocorre devido a um fator simples: a informação tem se caracterizado como o principal ativo da maioria dos negócios. Seguir o fluxo dos processos quase sempre significa seguir o fluxo das informações.

Considere a seguinte situação: identifica-se em um banco de dados um conjunto de informações incorretas. Existem no mínimo três formas de inserção de dados neste banco – cadastro pessoal, cadastro telefônico e cadastro realizado por certa empresa terceirizada. Como identificar qual das formas de inserção não estão atendendo à política de integridade? Talvez o problema ocorra apenas com cadastros telefônicos. Como aplicar os controles de segurança da forma correta, evitando sobrecarregar os processos de cadastro que não representam ameaça?

O paradigma de que garantir a segurança da informação reside exclusivamente na garantia da confidencialidade, da integridade e da disponibilidade está para ser quebrado. Não defendo que a visão original está incorreta, entretanto apresento um conceito que vem sendo amplamente discutido entre os profissionais de segurança do mundo todo, principalmente na Europa. Outros conceitos também bastante discutidos são a necessidade de garantia da autenticidade e a legalidade das informações. É importante não se prender exclusivamente à confidencialidade, integridade e disponibilidade.

A questão que deve ser considerada é: como garantir a confidencialidade, a integridade e a disponibilidade das informações sem conhecer detalha–damente a forma com que essa informação se relaciona com os processos de negócio? Qual é o grau de confiança das análises de risco, levando em consideração as complexas relações e caminhos que a informação assume dentro de uma organização ou entre organizações? Não seria necessário inicialmente disseminar uma cultura de controle total e rastreabilidade sobre a informação para depois garantir a adequada aplicação de segurança em suas diversas etapas de relacionamento?

Em resumo, sem conhecer os caminhos e formas da informação torna-se complexo garantir a sua confidencialidade, integridade e disponibilidade. Divulgar nas diversas áreas da organização o que significa rastreabilidade e exigir sua aplicação irá permitir o aumento da segurança, uma vez que é sensivelmente mais simples proteger o que se controla. É fortemente aconselhável divulgar através da organização o conceito de rastreabilidade e exigir que as diversas áreas da empresa interajam propiciando links adequados que irão facilitar os processos de segurança.

Input

CONCEITO

HACKER
Que bicho é esse?

Por: Koiti Egoshi | koiti@egoshi.com.br

Este artigo tem basicamente dois objetivos: em primeiro lugar, fazer distinção clara entre hacker e cracker, termos utilizados por aí, como se fossem um sinônimo do outro, o que não corresponde à verdade – daí, tem contribuído para denegrir a imagem do hacker. Em segundo lugar, listar as "subespécies" cracker e hacker que habitam e atuam no Cyberspace(1).

O que significa literalmente HACKER ?

Literalmente significa machado de abrir brecha nas árvores, para extrair seiva. Mas, a disseminação do uso do termo hacker deve-se a programadores aficionados do MIT – Massachusetts Institute of Technology, que nos Anos 60, se autodenominaram hackers(2).

Origem da compreensão e utilização pejorativa da palavra HACKER

Em 1988, o hoje famoso e polêmico âncora Dan Rather, da TV CBS nos Estados Unidos, chamou hackers de terroristas que pretendiam dominar todos os computadores da Terra, ao relatar sobre uma conferência de aficionados por computadores. A partir daí, espalhou por aí, que hacker é maléfico.

A quem podemos chamar de HACKER?

Genericamente por aí, chamam de hacker a qualquer um que é aficionado por computadores.

Popularmente Hacker é o cracker que invade sistemas alheios e os prejudica de alguma forma.

Juridicamente, é hacker mocinho ou bandido, conforme suas intenções e resultados de suas ações, serem qualificadas para o mal ou para o bem, pelo julgamento e justiça dos homens. hacker mocinho poderá ser reconhecido como simplesmente hacker. hacker bandido poderá ser enquadrado como cracker.

Tecnicamente, é hacker qualquer agente que tem pelo menos um razoável domínio sobre Lógica e Linguagens de Programação, Sistemas Operacionais e Redes de Computadores.

Os programadores aficionados do MIT – Massachusetts Institute of Technology, que nos anos 60, se autodenominaram hackers, como vimos anteriormente, tinham pelo menos um razoável domínio sobre Lógica e Linguagens de Programação e Sistemas Operacionais, além de estarem implementando na época as primeiras Redes de Computadores, para o progresso da humanidade.

Portanto, hacker é aquele técnico benfeitor aficionado por computadores em rede. A um hacker altamente capacitado tecnicamente, chamamos de white hat.

Quem pode ser tachado de CRACKER?

Qualquer um aficionado por computadores, que invade sistemas alheios e os prejudica de alguma forma. Suas intenções e resultados de suas ações poderão ser classificadas como perniciosas pelo julgamento e justiça dos homens, e daí, poderá ser enquadrado como criminoso. A um cracker altamente capacitado tecnicamente chamamos de black hat.

ENTRE WHITE HAT E BLACK HAT

Listamos a seguir algumas "subespécies" cracker e hacker:

SNEACKER

Hacker ou cracker contratado por uma empresa para descobrir vulnerabilidades e aprimorar segurança nos sistemas.

SCRIPT KIDDIE

Cracker inexperiente em programação, mas de razoável experiência prática em invasão de computadores, através de scripts e utilitários disponíveis no mercado. A grande maioria dos crackers é constituída de Script Kiddies.

LARVAL STAGE ou SPAWN

Um agente de nível técnico elevado, que é quase hacker.

WANNABE

O nome é em alusão aos fãs da Madonna. É um indivíduo que deseja ardentemente ser um hacker, custe o que custar. Tanto pode ser um newbie quanto um quase larval stage, que já leu e estudou muito.

LAMER

Um newbie ou luser, que não sabe ou não tem condições de saber como funciona, mas quer invadir computadores alheios, não importa como. Lame significa aleijado ou manco.

NEWBIE

Iniciante ingênuo com muita fome de aprender a acessar computadores alheios. Corre o risco de "entrar de gaiato" e daí, poderá vir a ser enquadrado como cracker.

PHRAEKER

Cacker de sistemas telefônicos ou, os primeiros crackers.

LUSER

É aquele que não quer aprender nada, a não ser operar o computador para divertir-se ou obter o que lhe interessa. Geralmente, está mais perdido na rede que peixe fora d'água. Mas pode se dar mal, e ser enquadrado juridicamente como cracker.

CARDER

Cacker especialista em fraudar cartões de crédito.

WAR DRIVER

Cacker especialista em wireless(redes sem fio).

WAR CHALKER

War Driver que desenha com giz/tinta um lugar propício para operação de war drive. A prática dessa idéia nasceu do Web Designer Matt Jones em Junho de 2002. Mais informações em : www.warchalking.org.

FUCKER

Hacker que sente o maior orgasmo detonando máquina alheia.

ARACKER

Hacker "de araque", cheio de conversa mole; do que fala, quase nada sabe fazer.

O PERFIL TÉCNICO DE UM WHITE HAT E BLACK HAT

Domínio sobre:
Raciocínio Lógico-Analítico: Lógica de Programação
Conhecimento Teórico e Prático: Linguagens de Programação
Raciocínio Lógico-Analítico: Lógica de Sistemas Operacionais
Conhecimento Teórico e Prático: Sistemas Operacionais
Conhecimento Teórico e Prático: Telecomunicações
Conhecimento Teórico e Prático: Redes de Computadores
Conhecimento Teórico e Prático: TCP/IP e outros Protocolos de Comunicação
Conhecimento Teórico e Prático: Plataforma e Arquitetura de Hardware e Software

O ESPíRITO DO HACKER

O "Espírito de hacker" era uma questão de estratégia competitiva entre jovens e brilhantes estudantes e profissionais dos anos 60 no MIT, como destacamos anteriormente.

Posteriormente, nos anos 70, empresas mais competitivas contratavam profissionais com esse perfil, e até criavam grupos específicos só para "fazer o sistema cair", descobrir *bugs* e assim, aprimorar a segurança de sistemas. Bill Gates e Paul Allen foram dois desses primeiros *hackers* profissionais, que faziam parte do Grupo de Programadores de Lakeside, tipo de um Clube do Bolinha, que eles com outros amigos criaram dentro do aristocrático colégio de mesmo nome.

Já em 1968, eles acessavam minicomputadores DEC/PDP-10 – ou Digital Equipment Company/Program Data Processor-10, blocados pela General Electric à Lakeside. Mais tarde, Bill Gates e Paul Allen foram contratados pela C3 - Computer Center Corporation ou C ao Cubo(como preferia chamar Bill Gates, essa empresa que foi fundada em 1968), para trabalharem no turno da noite, para fazer o sistema cair. A C3, coincidentemente, havia passado a oferecer block-time ao colégio Lakeside, aquele mesmo onde ele estudava. Assim, Bill Gates chegou até a acessar os arquivos contábil-financeiros da C3 e reduzir as horas de uso de block-time dele próprio – nesse caso, ele deu uma de cracker e quase foi incriminado como tal. Hoje, mais do que nunca, esse espírito de hacker continua vivo como uma chama ardente.

O JEITÃO DE SER HACKER

Tecnicamente

Hacker é um programador,

que quer cada vez mais testar, simular, entender e controlar a máquina. Feito professor Pardal, desafia a si mesmo para criar uma máquina "que faz tudo e que seja à toda prova".

A idéia de "colocar uma máquina à toda prova" é seu grande desafio, e a conquista da máquina que "faz tudo" é a sua maior glória.

Psicologicamente

Hacker é um "moleque de rua" menor ou maior de idade, que usa estilingue com mamona só para se divertir de mocinho e bandido. É curioso, amante e fuçador de computador. Gosta de brincar, estudar e fazer relax, trabalhando livremente e sem formalidades. Apela para a total liberdade de ação no trabalho, igualdade em acesso e fraternidade na troca. Computador para ele é um parceiro inseparável de diversões;

É incrivelmente prático, mas também sabe planejar feito administrador. É anárquico, informal, da contracultura e faz questão de ser chamado de você;

É criativo. É movido à adrenalina, tem espírito aventureiro e vive de desafios.

É inconformado com a situação e busca o progresso.

É individualista, mas troca idéias com outros, e até participa com demais vez e outra, principalmente com a sua "tribo".

Compartilha abertamente com outros suas idéias, criações e invenções, como também usufrui de contribuições de outros. Mas detesta ser "maria vai com as outras" e daí, evita tanto quanto possível fazer algo junto com os outros.

Curte a liberdade, o auto conhecimento, o livre-acesso, o livre-pensar, o livre-agir.

Mais do que ganhar dinheiro, o importante é curtir a vida e ser feliz; então diz não, ao autoritarismo.

Agnóstico, ateísta e neo-pagão. Quando não está hackeando, está jogando um game ou assistindo a um filme de ficção científica no computador.

Para hacker, todo dia é dia de diversão, seja trabalhando, estudando ou fazendo outras coisas, porque existe o computador, esse brinquedinho maravilhoso, fantástico e fascinante.

Quando não está no computador está treinando Artes Marciais, para malhar o corpo, sentir melhor o coração e desanuviar a mente.

Ou meditando Zen feito bobo defronte à parede, para pegar no ar novas idéias criativas.

Ou curtindo uma musiquinha crazy para relaxar. Filsófica e sociologicamente hacker é um elemento fora do mundo formal da era industrial, embora seja um rebento dela e usufrua seus benefícios. Está acima do Estado, das empresas e dos grupos.

Está acima dos conceitos de bem e do mal das religiões. Acima da discriminação de raças, credos, nacionalidades e posições sociais. Hacker é individualidade, liberalidade e fraternidade manifestas.

Hacker, embora individualista, não é egoísta. Busca incessantemente a liberdade, igualdade e fraternidade entre povos.

AS FORÇAS MOTIVADORAS MAIS OCULTAS DE UM HACKER OU CRACKER

Desejo de vencer desafios.

Espírito de aventura movido à adrenalina.

Lei do menor esforço ou obtenção de vantagem em tudo – Lei de Gérson.

Vontade de ganhar dinheiro.

Molecagem – brincar de bandido e mocinho; travessura.

Curiosidade, exploração do desconhecido e busca incessante da fórmula, para chegar lá. Gosto por criar, experimentar sua criação, comprovar sua funcionalidade e dar o grito da vitória. Vontade de detonar.

Notas:

(1) Sobre os mais variados agentes do Cyberspace, consultar www.jargonfile.com.

(2) Conforme citado por Pekka Himanen no seu livro *A ética dos HACKERS e o espírito da era da informação*, publicado pela Editora Campus.

Gestão

PLANEJAMENTO

Plano Diretor

Agenda de Segurança da Informação

A conjuntura atual nos coloca em uma posição de estruturar e planejar tudo que é relacionado à•a segurança. Este é o momento de reflexão, momento em que devemos sopesar ações passadas considerando a sua eficiência, e as ações futuras levando em conta seu relacionamento com os aspectos estratégicos para o negócio. Não considero que a responsabilidade pela definição do Plano Diretor de Segurança da Informação – PDSI, seja exclusiva da área de tecnologia, deveria ser uma ação conjunta à Alta Administração, mas no Brasil na maioria dos casos é assim que funciona. Como estou preocupado, mais com a prática do que com a teoria, este artigo versará nestes moldes. Para garantir um artigo sintonizado com as últimas tendências utilizei como referência o guia do SGSI da BS 7799-2 e também a experiência de alguns dos maiores gestores de TI do país, com quem tenho relacionamento.

Por F. F. Ramos - Axur Information Security

http://www.axur.com.br/

Gestão

PLANEJAMENTO

Nosso primeiro passo será listar todos os projetos relacionados à segurança que foram realizados no ano corrente. Não se pode planejar o futuro sem entender o passado, pois seria incoerente tratar de novos desafios sem antes dar o fechamento àquilo que foi realizado ou está em fase de finalização. Com base em nosso planejamento passado devemos aferir nossa capacidade de predição orçamentária considerando também a previsão de tempo, recursos e expectativas. Vou lhes contar uma regra de ouro da segurança, que parece óbvia mas nem sempre é seguida: só o que é monitorado pode ser medido, só o que é medido pode ser gerenciado. Se não houve histórico para determinarmos a performance de determinada ação, dificilmente saberemos se estamos indo para o lado certo.

Todo o investimento em um controle de segurança deve ser justificado com a minimização de um risco.

Conceitualmente "controle de segurança" é tudo aquilo que se aplica na redução de determinado risco. Controles são firewall, IDS, biometria, redundância de link etc

Quanto gastar no controle? A análise de risco é quem vai dizer. Se comprei um firewall e não consigo mensurar através de informações gerenciais qual o impacto da sua ausência no negócio da minha organização, entã, não posso afirmar que eu preciso de um firewall. Lembro que esta análise deve ser preferencialmente financeira, em alguns casos – pela dificuldade que ainda temos em tangebilizar o valor do ativo informação – está a contento uma análise qualitativa apresentando o impacto da quebra da confidencialidade, integridade e disponibilidade.

Agora vamos ao que realmente nos interessa: quais são as melhores práticas para a confecção de um plano diretor anual para uma empresa de médio e grande porte. Preparei uma lista de projetos que não consideram contratação de hardware ou software, porque assim eu entraria em particulares que variam dentro de um grande espectro. Refiro-me àquilo que é imprescindível e que independente da natureza do negócio, deve ser realizado, variando apenas o escopo abrangido por cada um dos tópicos.

Primeira Reunião com Fórum de Segurança: esta reunião, que deve contar com a parcitipação da Alta Administração da organização, proverá direciona–mento ao processo de segurança da informação, garantindo apoio à política de segurança existente e apontando quais são os níveis de risco aceitáveis para a organização.

Elaboração do calendário:

Janeiro/ Fevereiro

Análise de Riscos e Vulnerabilidades: é imprescindível que seja realizada uma análise de riscos e vulnerabilidades. Se já foi realizada uma análise no ano anterior, então é o momento de revisá-la.

Esta análise deve retornar como produto um relatório que será utilizado pelo gestor durante todo o ano. O relatório de análise de risco é dinâmico e deve receber como anexo as demais análises realizadas pontualmente sobre processos que foram agregados ao negócio da organização durante o ano.

Março

Revisão e Confecção dos Procedimentos Operacionais e Normas de Segurança: para que haja aderência do processo de segurança à norma BS 7799-2, faz-se necessária a documentação de todos os procedimentos operacionais e normas de segurança que garantirão a efetividade dos controles implementados. Este trabalho deve ser realizado por uma equipe especializada, uma vez que nem sempre a maneira como está sendo realizado o rodízio das fitas de backup ou o rótulo das informações, por exemplo, é o mais correto. A participação de uma equipe especializada facilita a padronização das regras seguindo os critérios das melhores práticas em segurança.

Abril

Primeiro Teste de Intrusão Externo: é indicado que sejam realizados pelo menos dois testes de intrusão em empresas que possuem endereço IP válido na internet. Após a implementação dos primeiros controles sugeridos na análise de risco que deve ter sido realizada no início do ano, já é momento de auditar através de tentativas simuladas de ataque a partir da Internet. Se a empresa já possui um plano de continuidade, é interessante considerar ataques de denial-of-service (esgotamento de recursos) e ensaiar a equipe de resposta a incidentes. Não se assuste quando eu escrevo "equipe de resposta a incidente", independente do tamanho da organização deve haver alguém responsável por responder de maneira efetiva quando identificado um ataque: não importa que seja uma "equipe" de um só homem, de dez pessoas ou que seja um serviço terceirizado – como um CIRT, por exemplo.

Maio/Junho

Auditoria Tecnológica: para que haja um endosso mensal, garantindo que a empresa mantenha o nível de segurança alcançado através da implementação dos controles sugeridos na análise de risco e delineados na estratégia de continuidade. Todos os controles tecnológicos devem gerar registros e estes registros devem ser verificados. A auditoria tem o caráter de envidenciar oportunidades de melhoria dentro da organização. A norma BS 7799-2 sugere que esta auditoria seja realizada por uma equipe independente e especializada, participando também o auditor interno.

Julho/Agosto

Treinamento de Funcionários: imprescindível é o treinamento dos funcionários da organização. É interessante que sejam realizados seminários tratando de temas como: Engenharia Social, Importância do Backup, Cuidados com a Senha, Classificação da Informação etc. Em casos peculiares, considerando a participação da Alta Administração, devem ser agendados treinamentos tratando da proteção de notebook, utilização de criptografia e assinatura digital ou qualquer outro assunto que possa auxiliar à redução de risco, conforme índice indicado pela própria Alta Administração como aceitável na matriz dos riscos.

Atualização / Treinamento do Security Officer: é tempo de atualização frente ao vasto contingente de conhecimentos que se renovam. O Security Officer ou quem for que ocupe a função de gerenciar a segurança da informação – seja este um analista, gerente, diretor ou até mesmo alguém que acumule esta função -, deve realizar pelo menos um treinamento anual para reciclagem. Este treinamento tem por objetivo o intercâmbio de boas idéias com os colegas de outras organizações e também a reflexão das melhores práticas de segurança, considerando o conhecimento e a experiência dos instrutores. Deve ser analisada também a possibilidade de um treinamento de Security Officer para uma equipe inteira, em treinamento in company. Esta prática vem sendo cada vez mais freqüente e tem trazido ótimos resultados.

Setembro

Evento Interno de Segurança da informação: para que haja o comprometimento da organização como um todo, em diversos momentos é necessário realizar trabalhos de reforço à Política de Segurança. Muitas empresas optam por adotar um dia do ano como Security Day – Dia da Segurança da Informação, e aproveitam esta data para o lançamento da sua campanha de segurança, com camisetas, mousepads, pronunciamento do presidente etc. O assunto segurança não é dos mais amigáveis. Apresentar novos controles ou conceitos que parecem tão cerceadores em um coquetel ou utilizando o recurso de um mascote, pode ser uma boa idéia.

Outubro

Segunda Reunião com Fórum de Segurança / Análise Crítica da Política de Segurança: para esta reunião é interessante que seja organizado uma espécie de Security Scorecard com indicadores de controle para cada risco tratado. Para que haja o giro do PDCA do sistema de gestão de segurança da informação, faz-se necessária uma revisão crítica da Alta Administração para endossar a continuidade da Política de Segurança da Informação.

Novembro/ Dezembro

Entrevista de Aderência à Política de Segurança: a entrevista de aderência à política tem como objetivo medir a cultura de segurança da informação dos funcionários. É uma espécie de termômetro que fornece indicadores para que seja providenciado um acerto de rota. Caso seja evidenciado, por exemplo, que o departamento de engenharia está conhecendo pouco da política de backup, então entra em ação a equipe de endomarketing, sugerindo cartazes ou treinamentos específicos para elevar o conhecimento destes funcionários a um nível considerado adequado. Existem diversos softwares que realizam avaliação dos funcionários, deve-se considerar a compra ou contratação deste tipo de serviço.

Encerramento

Segundo Teste de Intrusão: é recomendado que sejam realizados no mínimo dois testes de intrusão por ano. Em algumas organizações recomenda-se testes trimestrais. Quem decide? Os interesses da organização em vista da análise de risco.

Além dos pontos listados acima é necessário que sejam realizadas atividades mensais, que garantam a manutenção da segurança. Uma boa prática é a realização de chekups mensais na forma de auditoria para garantir que o nível de segurança está sendo mantido. Deixe reservado um fundo que possa cobrir eventuais consultorias em uma média de 30 a 50 horas mensais, considerando a possibilidade de ocorrerem eventos pontuais que necessitem da ajuda de consultores experientes, como uma análise forense ou uma análise de vulnerabilidades em uma nova tecnologia.

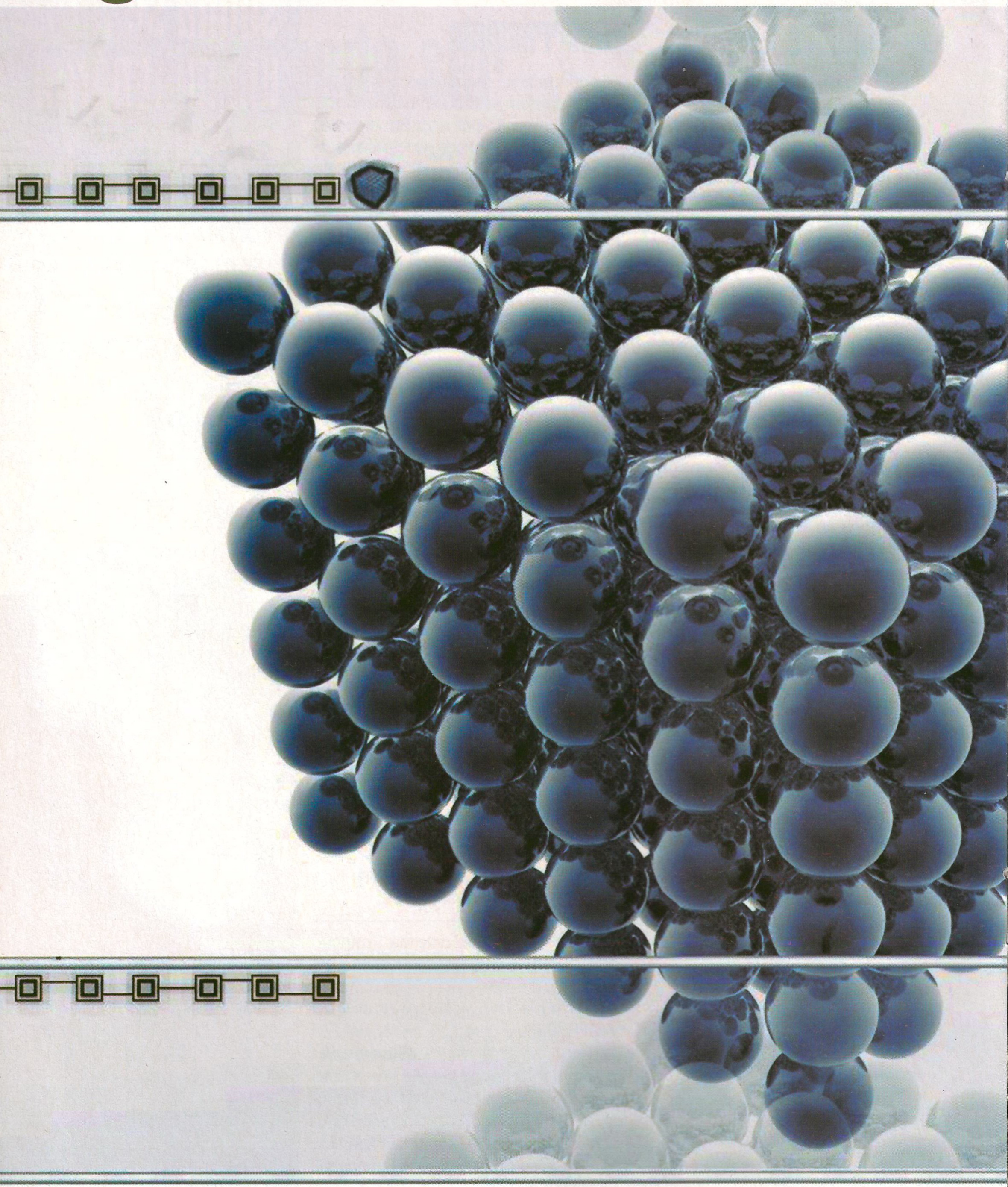
A tecnologia da informação nos faz subir cada vez mais na escalada onde cada centímetro de vantagem nos dá maior participação em mercado, satistação do cliente e diferenciação. Nesta escalada não podemos subir, subir, subir sem pensar em segurança. Entenda os 127 controles apresentados na ISO 17799 como aquele pino que os alpinistas prendem à parede a cada metro de subida, garantindo que se houve algum tipo de queda, esta será controlada e estará dentro do limite de risco aceito. Espero que este perfil de direcionamento para as atividades de segurança possa ajudá-lo a organizar as prioridades para o próximo ano. Este artigo não tem a intenção de ser um modelo a ser seguido, mas de ser utilizado como benchmark na hora em que você for confeccionar seu plano diretor.

Colaboradora freqüente da Proteção Hacker, a Axur é uma empresa brasileira especializada em consultoria e desenvolvimento de soluções para segurança da informação. Dedicada à geração e implementação de tecnologias de segurança, apresenta soluções com metodologia própria, nas normas ISO/IEC 17799 e Baseline Protection, utilizando o suporte tecnológico de produtos e ferramentas desenvolvidos pelo Tamanduá Labs. - laboratório com conceituação internacional.

www.axur.com.br

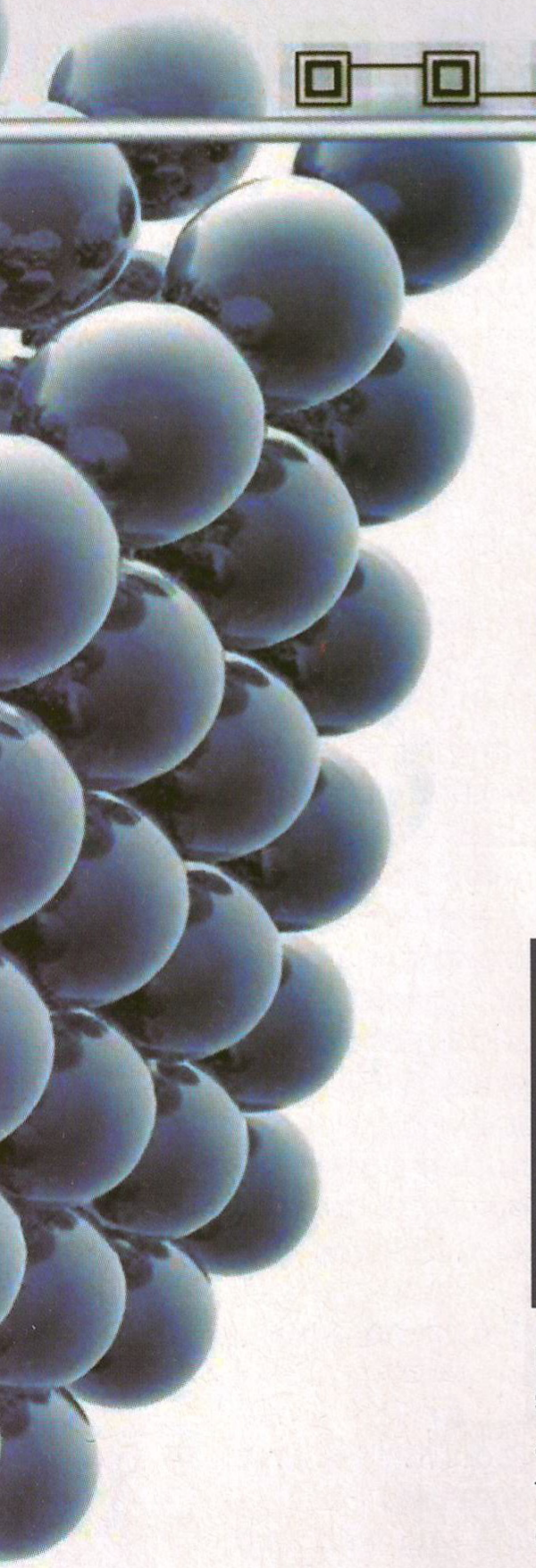
Hight Tec

GLOBALIZAÇÃO



Autor: Marco Filippetti

Netceptions Consulting www.netceptions.com.br



Convergência digital

Muito tem se falado sobre convergência. Mas afinal, qual o real significado por trás desse termo, que vem ganhando cada vez mais destaque na mídia? O surgimento de palavras e termos "modistas" não é um fenômeno restrito aos dias atuais. Lembram-se quando o termo "multimídia" começou a ser popularizado? Bastava um computador possuir uma unidade leitora de CD e uma placa de som para ser taxado de uma poderosa "estação multimídia"! Outro bom exemplo é o termo "globa lização", por alguns anos, o preferido de 11 entre 10 vestibulandos em suas redações. O que se dizer, então, do termo "realidade virtual"? Esse foi utilizado à exaustão, muitas vezes em contextos totalmente inconsistentes. A verdade é que nem todos conheciam o real significado destes termos, mas isso, realmente, não importava. Seu uso era perfeitamente justificável – e quase "obrigatório".

Afinal, eram esses os termos do momento! Imagine um vestibulando escrevendo uma redação que não mencionasse, em algum momento, o termo "globalização"!

Hight Tec

GLOBALIZAÇÃO

Voltando ao nosso assunto... o que seria, então, "convergência tecnológica"? Uma nova denominação para uma prática já há muito existente - a chamada "reinvenção da roda", ou uma definição para uma atividade realmente inovadora? Eu diria, um pouco de ambos.

A tão falada convergência tecnológica vem sendo o objetivo principal de muitas empresas, já há algum tempo. No passado, porém, a escassez de recursos tecnológicos limitava essa convergência à integração dos sistemas computacionais, resultando em uma "pseudo convergência". Não era possível (ou viável) a integração - convergência - entre determinadas tecnologias, notadamente telecomunicações e tecnologia da informação. No entanto, a pseudo-convergência era uma necessidade real, que abriu uma enorme janela de oportunidade. Através desta janela, algumas empresas identificaram um mercado altamente lucrativo. Foi quando surgiram as primeiras integradoras, empresas que se propunham a oferecer soluções completas para a integração de sistemas computacionais distribuídos. Ainda não era a real convergência tecnológica, mas um grande passo nessa direção começava a ser dado. Poucos anos depois, com o excepcional avanço tecnológico nas áreas de comunicação de dados e teleinformática, a convergência tecnológica total tornou-se, de fato, plausível.

A real convergência tecnológica alia as mais avançadas técnicas de integração de sistemas computacionais distribuídos com os sistemas de telecomunicações modernos, ou legados.

O resultado é a integração total, a convergência real.

A inexistência de sistemas isolados. Vídeo, voz e dados, os três pilares das comunicações modernas, passam a coexistir no mesmo meio, no mesmo ambiente de transporte (ou, usando um jargão da área, no mesmo "tubo").

Não mais é necessária a manutenção de uma rede de telecomunicações em paralelo com uma rede de comunicação de dados. Ambas as tecnologias passam a trafegar pelo mesmo meio. A primeira grande vantagem que a convergência total apresenta é a dramática redução nos custos com telecomunicações, uma vez que voz e dados dividem os mesmos circuitos e tecnologias, e assim sendo, impulsos telefônicos simplesmente deixam de existir, reduzindo o custo de uma ligação interurbana ou mesmo internacional ao custo de uma ligação local (ou menos). Para comunicação inter-corporações (ex.: matriz – filiais), a economia pode ser ainda maior.

Outra grande vantagem é o barateamento e conseqüente utilização cada vez maior de sistemas de videoconferência, cujas informações também dividem a mesma rede unificada. A aplicação de tais sistemas reduz em mais de 70% a necessidade de deslocamento de executivos, resultando em uma grande economia para empresas que utilizam tal tecnologia. Essas são apenas algumas das vantagens que a convergência total pode trazer. Na verdade, a real convergência possibilita um número quase infinito de produtos, serviços e benefícios.

Como qualquer tecnologia recente, o desafio da convergência total é grande. Muitas das tecnologias empregadas no processo são ainda pouco conhecidas, outras acabam de ser tecnicamente dominadas, mas ainda são economicamente inviáveis. É o caso da manipulação dos comprimentos de onda dentro de fibras ópticas (DWDM – Dense Wavelenght Division Multiplexing), dos novos produtos que surgem a cada dia no mercado, dos inúmeros protocolos de comunicação que foram criados ou modificados nestes últimos anos – como o MPLS (Multiprotocol Label Switching) e o IPv6. É preciso manter-se constantemente atualizado – com uma freqüência quase diária - na área para ser capaz de oferecer produtos e serviços de convergência que sejam competitivos e que satisfaçam as necessidades do cliente mais exigente - e manter-se

atualizado com essa intensidade custa caro. Outro grande problema – talvez o maior – é o complexo processo migratório dos sistemas já implantados (sistemas legados) para o sistema convergente (também conhecido como "Sistema NGN" ou "Sistema de Próxima Geração").

No mercado atual, poucas são as empresas de tecnologia que ousam anunciar o oferecimento de um pacote realmente completo de soluções em convergência tecnológica. E as poucas que o fazem, com raras exceções, ainda não estão realmente preparadas para entregar estes serviços. Por esta ser uma área ainda pouco explorada – e portanto, pouco conhecida - pouquíssimas empresas hoje são privilegiadas com todos os benefícios que essa tecnologia pode oferecer. As poucas empresas que se encontram adiantadas no processo de adoção do Sistema NGN já são capazes de sentir o "peso" da mudança: Sensível redução dos custos com manutenção e operação dos sistemas, disponibilidade para dedicação em tempo integral ao "core business", sensível aumento de receitas e lucros, maior controle operacional, e desenvolvimento de produtos e serviços de melhor qualidade a custos reduzidos.

Esses são apenas alguns dos "efeitos colaterais" gerados pela adoção de soluções realmente convergentes.

Hoje, a transmissão de voz ainda responde pela maior fatia da receita das operadoras de telefonia. Projeta-se, no entanto, que dentro de 5 anos, a transmissão de dados já será responsável por mais de 70% da receita obtida. Isso mostra a popularização de tecnologias convergentes como Vo"X" (Vídeo e/ou Voz sobre IP, Frame relay, xDSL, ATM, etc.), QoS (Qualidade de Serviço), áudio e vídeo "streaming" etc.

A pesquisa e o desenvolvimento de novos padrões (como o padrão HDTV – *High Definition TeleVision*), novas aplicações, e novos protocolos de comunicação visando o aumento de performance das redes de dados – aumento este necessário às novas aplicações – tem acontecido em alta velocidade. Hoje, a atenção das grandes corporações e dos "early adopters" (empresas que estão na dianteira tecnológica) volta-se para um novo protocolo (mais um!) conhecido até o momento como FastTCP. Este protocolo de transporte – derivado do TCP, do conjunto TCP/IP – conseguiu em testes de laboratório uma performance infinitamente superior ao seu "primo", o TCP, possibilitando a transmissão de vídeo de alta definição em questão de segundos:

(http://netlab.caltech.edu/pub/papers/fast-030401.pdf).

Dentre os "early adopters" que estão testando este protocolo em ambiente de produção, destaca-se a Disney, que está aplicando o mesmo em seus parques temáticos para transmissão de vídeo em tempo real em telões espalhados pelos mesmos. Os testes comprovam: é uma questão de tempo para que mudemos do padrão TCP/IP, para o padrão de próxima geração FastTCP/IPv6.

O grande problema, por enquanto, ainda é a qualidade do acesso (enlace) que atende os usuários finais – também conhecida como "última milha" (*last mile*), que em quase 100% dos casos ainda é feito através de par metálico (cobre). As novas tecnologias requerem fibra óptica.

Acredito que, a partir de 2004, começaremos a presenciar cada vez mais a aplicação de tecnologias verdadeiramente convergentes. E quando essa convergência – a verdadeira! - for uma realidade cotidiana poderemos, finalmente, entender o real significado por trás de termos como multimídia, globalização etc... .

Por Marco A. Filippetti
Sócio-diretor da Netceptions Consulting.

(www.netceptions.com.br).

Vírus

ANÁLISE DE CASO

A VERDADEIRA FACE DO VÍRUS MYDOOM

Era uma vez um "Vírus" chamado MyDoom...

Equipe Proteção Hacker

É dia 26 de janeiro de 2004, 7:30 da manhã. Uma colega de trabalho, ao chegar, dizia-me tempestuosamente: "Você já viu o novo vírus, acabei de escutar na rádio a notícia...".

Sim, a partir desta data alguém auto-intitulado "Andy" anunciava ao mundo que o mercado negro dos vírus de computadores realmente existia... E pelo jeito paga-se bem por um vírus bem-feito.

Não era apenas mais um vírus, era simplesmente um desafio completo a todo tipo de "política de segurança" já pensada por todos nós, envolvidos diretamente com aspectos de TI, e enquanto "Andy" dizia: "Me perdoem, mas estou apenas fazendo meu trabalho", todos nós nos perguntávamos: "porque alguém criaria um vírus e em seguida pediria desculpas no código do mesmo?". Sim, esse alguém com certeza não estava feliz com as linhas embutidas em "seu" Worm, ou não (como diria Caetano Veloso)!

Vírus

ANÁLISE DE CASO

Chuva de verão

Parece que o vendaval W32/MyDoom.A e W32/MyDoom.B, ou simplesmente MyDoom para os mais íntimos, já foi embora... E não deixa saudades!

O vírus, sob a classe Worm que além de MyDoom também é conhecido como Novarg, Shimg e MIMAIL, inundou os servidores de e-mail de todo o mundo e contaminou mais de 2 Milhões de computadores em apenas dois dias, estando inicialmente o Brasil entre os 7 países mais afetados, apareceu em nossos mailbox´s exatamente no dia 26 de janeiro de 2004. Guarde bem essa data!

A verdade nua e crua é que todo mundo especulou tudo o que podia e o que não podia. Podemos dizer que se extraiu o máximo de sensacionalismo do mesmo para vender jornais e conseguir ibope com notícias às vezes até "inventadas" sobre o "GNU/Vírus". Nessas horas, como dizem alguns jornalistas, "vale tudo"!

Vamos aos fatos de fato... o que é o MyDoom senão o primeiro vírus especulativo da história tal como o mais controverso, o primeiro vírus que possui fãs e adeptos, o primeiro vírus com propósito explicitamente definido, o primeiro vírus a explicar detalhes de sua criação, o maior vírus em nível de propagação com relação a tempo, o primeiro vírus a dar um prejuízo de 250 milhões de dólares ao mundo em apenas dois dias e finalmente, o primeiro vírus procurado "vivo ou morto" pela bagatela de 250 mil dólares!

Mas vamos à verdadeira face do vírus que prometia, conforme o próprio nome sugere, um verdadeiro massacre!! Foi diante desta enxurrada de especulações que a PH deste mês preparou um dossiê completo que você verá nas próximas páginas sobre o vírus que escreveu uma nova página na biografia da segurança da informação.

Fatos sobre o MyDoom

Muitas palavras e apenas uma verdade... ninguém sabe ainda explicar de onde veio o MyDoom. Alguns até especulam que o mesmo tenha sido criado na Rússia, mas o fato é que ninguém conseguiu provar nada até o presente momento (que tal jogar a culpa no Kevin Mitinick, no Bin Laden ou no Saddam Hussein só para não perder o costume?).

Na mesma segunda-feira ,cerca de 500 mil computadores em todo o mundo já estavam contaminados tal como já haviam sido detectadas aproximadamente 100 milhões de mensagens contendo o vírus. Na quarta-feira, 29 de Janeiro, este número já havia subido para 2 milhões de computadores infectados.

Para contaminar suas vítimas, o MyDoom, que na verdade trata-se de um vírus sob a classe Worm, chegava anexado a um e-mail que geralmente continha o subject "test" ou "status" sob as extensões .zip, .exe, .src ou .pif. com precisamente 29.189 bytes, onde os anexos .zip foram os mais relatados, mesmo assim, todos precisavam ser abertos/executados para que agissem no computador-alvo. Após a abertura, o vírus se autocopiava para o diretório "System" dos computadores e manipulava o registro dos mesmos para ser executado durante a inicialização do sistema (e não precisa nem lembrar que o MyDoom só infecta o sistema MS Windows).

O vírus também agia frente aos softwares antivírus instalados nos computadores infectados, não permitindo que os mesmos fossem atualizados após a contaminação. Segundo a própria Symantec, os usuários deveriam primeiramente deletar os arquivos infectados (ou utilizar alguma ferramenta de remoção especifica) para somente após atualizar seu produto, o conhecido e conceituado Norton Antivírus.

O grande problema é que o MyDoom, como todo bom Worm, utiliza-se da lista de contatos do próprio usuário infectado para se auto propagar, fazendo então com que outras pessoas conhecidas da vítima recebam o vírus, tornando então o remetente de certa forma "confiável".

Outro problema é que a princípio o Worm não fazia qualquer barulho, ou seja, ficava sem se fazer notar... isso, para conseguir cumprir seu principal propósito, sacudir os sites da www.sco.com e o da poderosa www.microsoft.com.

Especulações sobre o MyDoom

Propagar um vírus que se auto-execute em computadores Windows aproveitando-se de falhas de segurança do MS Outlook já não é fácil, agora, propagar maciçamente um vírus cujo anexo precisa ser aberto para que o mesmo seja executado é uma missão quase impossível...

Parece que todos de uma hora para outra se esqueceram dos princípios básicos no uso de mensagens eletrônicas, entre elas a de nunca abrir/executar anexos em mensagens desconhecidas ou suspeitas, nem mesmo arquivos .doc, pois como sabemos, podem conter o que denominamos "vírus de Macro".

Ainda assim, havia um fato no mínimo curioso. O W32/MyDoom.A, a primeira versão do Worm a ser relatada, estava na verdade programada para, do dia 1° de fevereiro ao 12° dia do mesmo, disparar ataques DOS (Negação de Serviços) em direção ao site da SCO Group (www.sco.com), e como o mesmo já se fazia presente em mais de 2 milhões de computadores, este ataque seria ainda pior, passando de um simples DOS para um complexo DDOS (Negação de Serviços Distribuída). Como já é de conhecimento público, a SCO Group Inc., proprietária do Unix Caldera, iniciou ainda no ano passado uma série de tentativas frustradas sob o propósito de processar e denegrir os criadores do GNU/Linux por fazerem uso de bibliotecas do mesmo Caldera na composição interna do sistema do Linux tal como empresas do porte da IBM, RedHat e Novel. Já em um segundo momento a mesma SCO ameaçou multar todos os usuários do sistema do pingüim simplesmente por o utilizarem conforme as normas da GNU, ou seja, gratuita e abertamente!

O buraco foi mais embaixo

O episódio acima, que ficou conhecido como a novela "SCO Vs. O Mundo", foi regido pelo Sr. Darl McBride, Presidente e principal executivo do SCO Group Inc., o mesmo que ofereceu U$ 250 mil para quem denunciasse o nome do criador do W32/MyDoom.A além de estar atuando diretamente com o Federal Bureau of Investigation (FBI) na tentativa de descobrir a identidade do mentor dos direitos intelectuais e principalmente judiciais do vírus!.

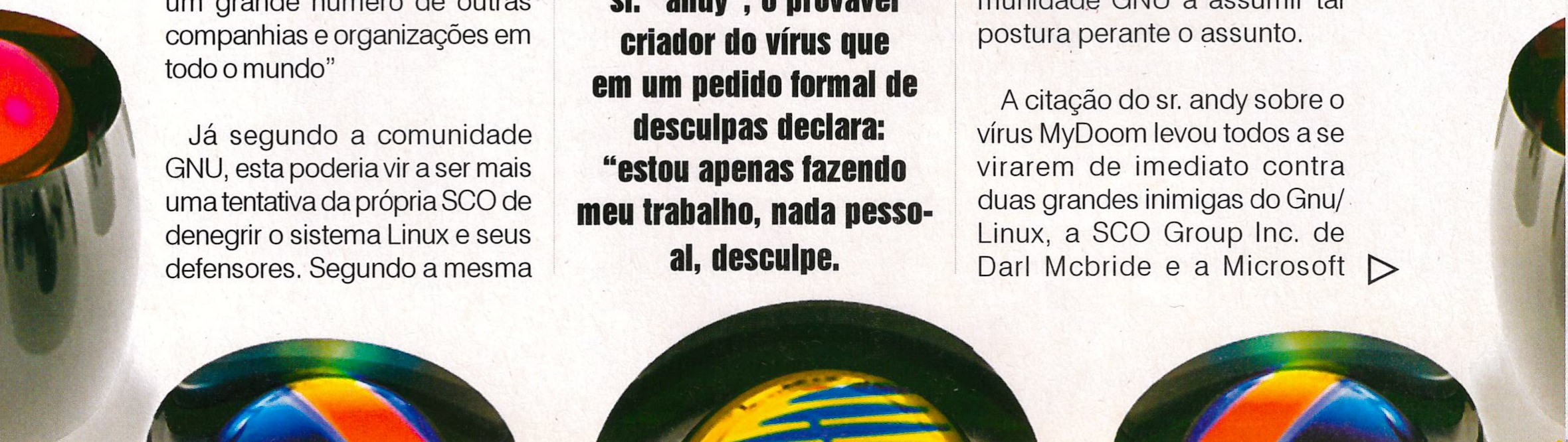
McBride declarou em entrevista a uma revista especializada norte-americana que a SCO tem sofrido atualmente muitos ataques do tipo DDOS a seu site, mas segundo o mesmo "Este é diferente e muito mais problemático, pois causa danos não só a nossa companhia como também a sistemas e produtividade de um grande número de outras companhias e organizações em todo o mundo"

Já segundo a comunidade GNU, esta poderia vir a ser mais uma tentativa da própria SCO de denegrir o sistema Linux e seus defensores. Segundo a mesma comunidade, depois de tudo o que a SCO fez para tentar inibir o uso e distribuição do Linux, o que impediria a mesma de propagar um vírus que atacasse a si própria para assim pôr toda a culpa na comunidade GNU?

Após a análise da segunda versão do vírus MyDoom, o MyDoom.B, descobriu-se em uma das linhas de seu código-fonte em forma de comentário a seguinte citação feita por um tal sr. "andy", o provável criador do vírus que em um pedido formal de desculpas declara: "estou apenas fazendo meu trabalho, nada pessoal, desculpe.

Mas sem dúvida o fato mais controverso de todos é exatamente o motivo que leva a comunidade GNU a assumir tal postura perante o assunto.

A citação do sr. andy sobre o vírus MyDoom levou todos a se virarem de imediato contra duas grandes inimigas do Gnu/Linux, a SCO Group Inc. de Darl Mcbride e a Microsoft ▷



▷ Corp de Bill Gates, afinal de contas, todos sabem que os hackers e programadores preferem o Linux, mas sabem também que nem só de pão vive o homem...Senão, por que um pedido de desculpas? Mas você deve estar se perguntando neste exato instante... A SCO vá lá, mas por que a Microsoft?

O fato é que o W32/MyDoom.B, ou seja, a segunda versão do MyDoom direcionava seus ataques não ao site da SCO, mas ao site da microsoft:: www.microsoft.com.

A mesma Microsoft como todos sabem é parceira ativa da SCO Group Inc. e que mesmo não possuindo participação direta no capital da SCO já adquiriu pelo menos US$ 12 milhões em licenças de seus produtos, sem contar o fato de nada nem ninguém possuir maior interesse em denegrir o Linux do que a gigante Microsoft.

E como termina a odisséia MyDoom?

Pra finalizar com chave de outro, o MyDoom. A cumpriu com o prometido, tirando então o site www.sco.com do ar e o tornando inoperante. A mesma SCO tratou logo de se prevenir e registrou dias antes do ataque o domínio www.thescogroup.com, para mostrar a todos que, mesmo frente ao MyDoom, a companhia ainda estava de pé!

Já o MyDoom.B fracassou diante do site www.microsoft.com, isso se deve ao fato de que a segunda versão do vírus acabou por não se propagar tanto quanto a primeira, tendo em vista que no Brasil não foram relatados casos de contaminação da versão "B" do vírus em questão (muito suspeito não??).

Entre aos prejuízos trazidos pelo MyDoom podemos destacar o lado corporativo da história, que mais uma vez somou custos no desenvolvimento de "N" aprimoramentos em seus mecanismos de defesa para intranets corporativas.

Já para aqueles que ainda não se livraram do MyDoom, estes poderão encontrar no CD da revista o arquivo FixNovarg.exe, que trata-se do software da Symantec que prometem detonar o verme de qualquer computador.

No mais, a vida continua... porque o Mydoom pode não ter durado muito tempo, nem ter sido tão devastador quanto se esperava-se que fosse, tampouco causado um verdadeiro massacre conforme prometia (com exceção do www.sco.com) e sequer representou uma grande dor de cabeça para as empresas fabricantes de antivírus e para os usuários da rede mundial de computadores. Mas existem alguns aspectos que o Mydoom conseguiu abordar com clareza tais como:

a) Qualquer empresa pode pagar para um "Andy" qualquer criar um vírus e com isso tirar um site de sua concorrente do ar por via de um ataque DOS;

b) Qualquer empresa pode pagar para um "Andy" qualquer criar um vírus que ataque seu próprio site e com isso acusar a empresa concorrente, denegrindo-a por completo;

c) Qualquer um pode escrever um vírus, pedir desculpas e em seguida gerar uma enorme especulação sobre a verdadeira origem do mesmo (pelo menos intelectual);

d) Fazer um Worm de contaminação em massa não é tão complicado quanto parece, basta saber um "feijão com arroz" em C++ para que criemos nossos próprios "massacres";

e) A Microsoft odeia o Linux, que odeia a SCO, que odeia o Linux, que odeia a Microsoft, que adora a SCO.

Todo o código no CD-ROM

Não muito contente, a PH foi muito além de abordar todas as informações já publicadas pela mídia sobre o Mydoom (que não foram poucas), mas resolvemos ir mais longe, e, com exclusividade, realizamos uma análise do código fonte do "temido" vírus, que está desnudo e completo no CD-ROM de encarte da Proteção Hacker. Tudo para que o mesmo nos sirva não somente para lembrarmos de atualizar o nosso antivírus, mas também como uma poderosa fonte de aprendizado...

"Muita" fumaça pra "muito" índio"

A revista Proteção Hacker entrevistou Koiti Egoshi, especialista em segurança para um parecer sobre esta praga e a política que a envolveu. No período em que foi feita a entrevista, o Mydoom estava em ativa propagação e a polêmica sobre o caso incomodava o sono da Microsoft e da SCO.

Por que ele é o mais avassalador de todos os tempos?

Calma, ainda não apareceu o mais avassalador! Sempre haverá um pior, algo que pode ir além das fronteiras técnológica digitais e tragam consequências realmente avassaladoras. Talvez esta seja a primeira praga anárquica, mas não a pior.

Por que ele foi uma grande ameaça, tecnicamente falando?

Na verdade, o famigerado MyDoomW32Novarg.A@mm ou W32/MyDoom-A é um WORM e não VíRUS*, que vem anexo com um e-mail. Depois que se instalar na sua máquina, ele ativa automáticamente um BACKDOOR (TROJAN HORSE), que em rede DRDOS - DISTRIBUTED REFLECTION DENIAL OF SERVICE, não só objetiva prejudicar SCO - que conforme expliquei em PROTEÇÃO HACKER Número 5, pode acabar com toda essa gracinha do Linux, como também por tabela, arranhar a Microsoft. Qual é a conseqüência? Fazer umas coceguinhas na SCO e na Microsoft, como também tornar a Internet lenta por mais alguns dias. Depois, tudo passa, como Sobig.F e outros passaram. Hoje, o MyDoom está na fase de triplicar a mesma mensagem para o mesmo destinatário. Talvez chegue a ponto de quadruplicar, e aí vai parar. Parar a Internet? Não. Vai parar de multiplicar, porque se continuar, a rede DRDOS, que até o momento é oculta, começará a ficar cada vez mais visível, e os crackers também. Tudo começa a ficar mais visível, à medida em que os espaços são preenchidos. Assim será um prato cheio para CIA, FBI e outros órgãos de CyberSegurança mapearem e identificarem o DRDOS e seus agentes.

O que ganhou seu desenvolvedor com isso?

No caso de MyDoom, a grande satisfação de ter atacado um monte de pedras e ter machucado a SCO.

Quando você não tem como contra-argumentar, você joga pedras, dá facadas, dá uns tiros, parte para a ignorância. Esse é o caso dos crackers fanáticos pelo Linux, que hoje sabem que tecnicamente, o Linux carrega uma parte proprietária do velho Unix que a SCO comprou da Novell, e esta por sua vez comprou da AT&T, conforme eu expliquei na PROTEÇÃO HACKER Número 5. Eles sabem, que juridicamente, podem perder o sorvete Linux.....

Você acha que a denúncia premiada é uma atitude correta?

É uma questão jurídica. O dia em que a porta de sua casa for arrombada e roubarem seus pertences, você fará um boletim de ocorrência na delegacia, certo? Melhor ainda se alguém aparecer e der os nomes dos criminosos, não é? Isso é denúncia premiada.

Tudo isso é balela. Se aparecer algum autor, será aquele doidão que quer se promover e ficar famoso. Na realidade são vários crackers em rede, se divertindo com DRDOS, usando worms, backdoors/trojan horses e outras praguinhas....

Koiti Egoshi

*Os especialistas como Koiti Egoshi diferenciam worm e vírus, mas este é um assunto pra outra Proteção Hacker...

Polêmica

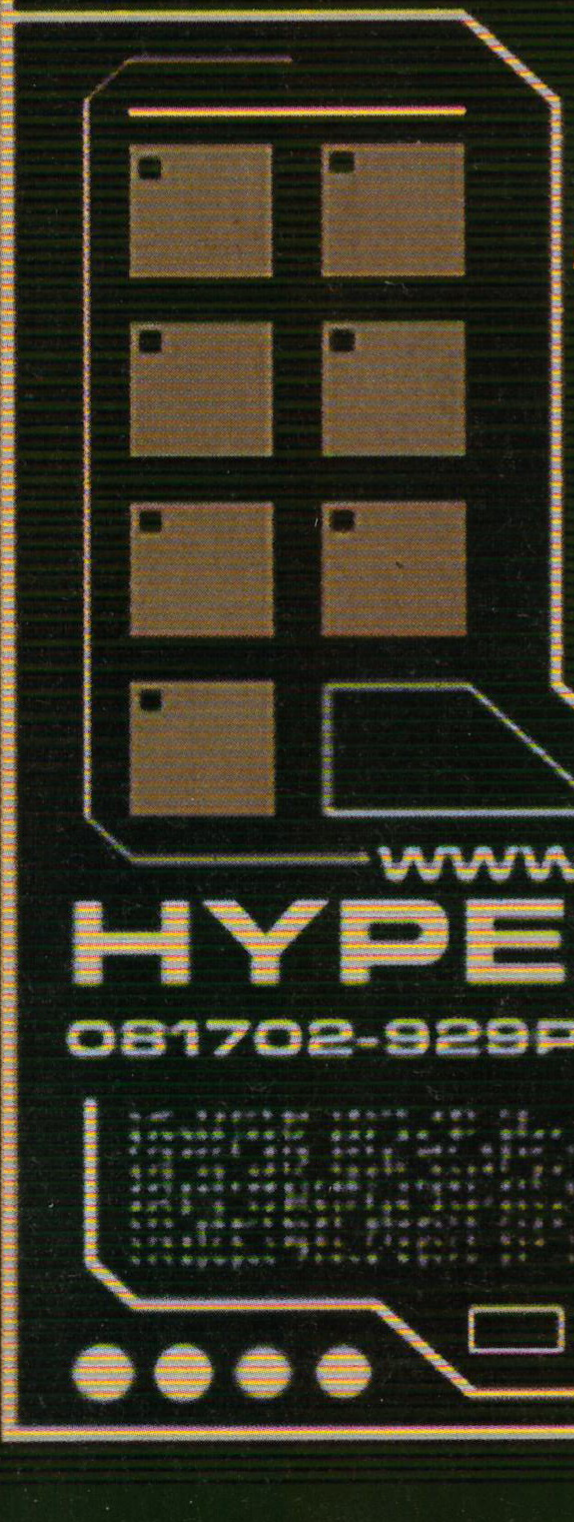
VISÃO HACKER

HaxOrs Lab INSIDE

Conheça a visão defacer das invasões

Uma guerra

A falha do CPanel 5



WWW.SYTHEON.COM

HYPERBOLE

081702-929P

USDL | Hacker

Sem Sentido

Polêmica

VISÃO HACKER

Caros leitores, espero que estejam gostando dessa série de matérias que estou escrevendo sobre o hax0rs lab, estou procurando dedicar mais tempo para escrevê-las de uma forma mais simples para um melhor entendimento dos leitores mais novatos. Gostaria de saber a opinião de vocês em relação à qualidade das matérias, vocês podem escrever para usdl@mail.com, que em pouco tempo irei respondê-los.

Abaixo irei descrever um pouco sobre o grupo, e algumas histórias que devem ser contadas ou como é o caso, recontadas.

IRC -(Internet Relay Chat)

Citarei aqui uma pergunta que foi feita a nós dias atrás, quando estávamos respondendo uma entrevista ao vivo para um canal de IRC, posteriormente publicada originalmente em http://www.ircmaster.com.br/textos.asp?sec=04&id=339; a entrevista consistia em duas séries de perguntas, as primeiras feitas pelos administradores do canal e a segunda pelos visitantes do canal, para a surpresa de alguns dos 150 visitantes que estavam presenciando a entrevista, um usuário que não se identificou nos fez a seguinte pergunta:

- Bom, uma vez vi um defaced(desfiguração de site) de vocês, e vocês colocaram uma mensagem muito estranha, um amigo meu que já trabalhou em Cuba me afirmou que aquilo era uma mensagem ao presidente Fidel Castro. Vocês têm algum envolvimento com a espionagem cubana?

Outrora, mais especificamente na edição nº6 da Proteção Hacker, eu comentei que o hax0rs lab é um grupo totalmente nacional, logo, não fazemos parte da espionagem cubana ou da espionagem de qualquer outro país.

Voltando ao meu artigo e deixando isso de lado, quero começar agradecendo e mandando um abraço para minha filha Ju, e ao Alexandre do meu trampo(MicroCamp/SP).

Alterando a ordem em que vocês estão acostumados nos meus artigos, começarei explicando o motivo do ataque e depois sobre a vulnerabilidade.

Com a mais recente guerra no Iraque, grupos de hacktivism* vêm intensificando ataques a servidores americanos e europeus desde 20 de março (Início da guerra).

Nós do hax0rs lab, não consideramos o grupo em si hacktivista, "f0ul" está nessa pelo conhecimento e diversão, eu(USDL) estou pelo conhecimento, desafio e quando posso uso isso para protestar.

Em julho de 2002 nós dois atacamos 500 sites para comemorar a marca de 900 sites invadidos.(Single IP**)

Em agosto de 2002 nós dois atacamos 1.158 sites para comemorar a marca de 1.000 sites invadidos.(Single IP**)

Em março de 2003, a mídia já colocava a dupla*(o grupo se mantém como uma dupla durante muito tempo, o que em alguns casos chamou a atenção da mídia que nos comparava com grupos que tinham 5 membros e agiam menos)* na liderança mundial de ataques digitais, sempre fomos contra a guerra, e levados pela ira de mais uma guerra estúpida e imoral, decidimos fazer alguma coisa que estivesse ao nosso alcance, em poucos dias nós conseguimos acesso a 7 servidores americanos que apoiavam a guerra, contabilizamos 8 mil sites.

Como esse ataque seria diferente dos outros e tinha como objetivo chamar a atenção para essa guerra sem sentido, eu me encarreguei de divulgar o ataque dias antes; Com isso, grupos que se sentem ameaçados por nós pelo fato de estarmos sempre na mídia, tentaram de todas as formas invalidar o ataque, fazendo um DDoS*** no site internacional de defacement mirror Zone-H****, mas não tiveram sucesso.

Como de praxe, nós fizemos pequenos programas para agilizar o ataque. Os servidores fo-

ram separados e ficaram 4 para mim e 3 para o f0ul, no dia houve um contratempo, e ele não pôde participar, e eu fiz o ataque nos servidores que eram de minha responsabilidade e que continham 5.000 sites.

Fiz um texto[1] padrão, e o coloquei em todas as páginas iniciais dos sites. Novamente foi tirado vantagem do fuso horário, e não havia nenhum administrador presente. A falha nos servidores se deu numa chamada ao arquivo guestbook.cgi, com username cpanel, algo já conhecido e usado pelos defacers. Porém a falha para conseguir root é bem restrita.

A falha se encontra apenas na versão do CPanel 5.

Cpanel é um painel de controle de web hosting, que permite ao cliente administrar sua conta com a interface web. A maioria de suas aplicações são escritas em perl e compiladas para binário.

A vulnerabilidade explorada

1) Execução de comando remoto no guestbook.cgi (/usr/local/cpanel/cgi-sys/guestbook.cgi)

Esta é uma clássica vulnerabilidade perl open function, que permite a qualquer usuário ler qualquer arquivo ou executar comandos como usuário válido do sistema.

Demonstração do conceito.

http://[Seu_site.com]/cgi-sys/guestbook.cgi?user=cpanel&template=|qualquer_comando|

2) Falha local (root)

Cpanel vem com pacote de openwebmail, um leitor de e-mails.

No sistema com suid perl instalado perfeitamente (com o modo suid ligado) um usuário local pode incluir seu próprio perl script quando rodar o openwebmail direto suidperl.

Openwebmail adicionará o perl include path(@INC) com a variável de ambiente SCRIPT_FILENAME, inclui então algum arquivo quando executado.

/usr/local/cpanel/base/openwebmail/oom line 14

```
if ( $ENV{'SCRIPT_FILENAME'} =~ m!^(.*?)/[\w\d\-]+\.pl! || $0 =~ m!^(.*?)/[\w\d\-]+\.pl! ) { $SCRIPT_DIR=$1; }
if (!$SCRIPT_DIR) { print "Content-type: text/html\n\n\$SCRIPT_DIR not set in CGI script!\n"; exit 0; }
push (@INC, $SCRIPT_DIR, ".");
.
.
.
require "openwebmail-shared.pl";
```

Demonstração do conceito.

I) Crie um arquivo openwebmail-shared.pl contendo o perl script que você deseja executar.

II) Ajuste o ponto SCRIPT_FILENAME para o trajeto do openwebmail-shared.pl que você acabou de criar.

III) Execute oom script (ex: suidperl -T /usr/local/cpanel/base/openwebmail/oom)

Solução rápida

I) Remova /usr/local/cpanel/cgi-sys/guestbook.cgi.

II) Desligue o modo suid no oom script (chmod 755 /usr/local/cpanel/base/openwebmail/oom).

* Uma mistura de hackers e ativistas, que fazem invasões para protestar.
** IP único, servidores diferentes.
*** Distributed Denial of Service, variante dos ataques DoS em que programas são instalados em muitos computadores e ativados ao mesmo tempo para um ataque coordenado.
**** Publica espelhos das invasões.

Até hoje já atacamos 5.000 sites em 4 servidores diferentes, mas não estamos comemorando nada, estamos protestando contra atos como a guerra de BUSH e BLAIR X SADDAM entre outras injustiças sociais e políticas.

hax0rs lab INSIDE por USDL

Agradecimentos: Ao pessoal da net, ArtNova, FHG, Mari, Meg, Paula, Felipe e Pla.

Wireless

SEGURANÇA

A evolução do WEP

WPA

tratamento especial às vulnerabilidades

Isabela Chaves Santos - UFRJ | Laboratório de Redes de Alta Velocidade (RAVEL)

O WPA, ou Wi-Fi Protected Access será o novo protocolo de segurança de camada de enlace para o padrão IEEE 802.11. Nesse artigo, a autora, que também é pesquisadora nessa linha, fala sobre o início da evolução do WEP, ou Wired Equivalent Privacy, o antigo protocolo, para o novo protocolo.

Ao longo dos últimos anos, pudemos observar um grande aumento no número de redes sem fio utilizadas por usuários caseiros, instituições, universidades e empresas.

Essa crescente utilização e popularização das chamadas WLANs trouxe consigo mobilidade e praticidade para seus usuários mas também trouxe uma preocupação com a segurança destas redes. É exatamente essa preocupação com a segurança das redes sem fio que vem fazendo com que os protocolos de segurança sejam criados, desenvolvidos e atualizados com uma velocidade cada vez maior.

WEP, a primeira barreira

O primeiro protocolo de segurança adotado, que conferia no nível do enlace uma certa segurança para as redes sem fio semelhante à segurança das redes com fio foi o WEP (Wired Equivalent Privacy).

Este protocolo, muito usado ainda hoje, utiliza o algoritmo RC4 para criptografar os pacotes que serão trocados numa rede sem fio a fim de tentar garantir confidenciabilidade aos dados de cada usuário. Além disso, utiliza-se também a CRC-32 que é uma função detectora de erros que ao fazer o "checksum" de uma mensagem enviada gera um ICV (Integrity Check Value) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho.

Vulnerabilidades do WEP

Após vários estudos e testes realizados com este protocolo, foram achadas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade.

No WEP, os dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta k de 40 bits ou 104 bits e um vetor de inicialização de 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k,v).

Porém, como no WEP, a chave secreta k é a mesma utilizada por todos os usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4 . Essa repetição de seqüência é extremamente indesejável, pois dá margem a ataques bem-sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

Além disso, há também uma forte recomendação para que seja feita a troca das chaves secretas periodicamente aumentando-se com isso a segurança da rede. Porém, essa troca, quando é feita, é realizada manualmente de maneira pouco prática e por vezes inviável, quando se trata de redes com um número muito alto de usuários.

E ainda uma falha do WEP constatada e provada através de ataques bem-sucedidos é a natureza de sua função detectora de erros. A CRC-32 é uma função linear e que não possui chave. Essas duas características tornam o protocolo suscetível a dois tipos de ataques prejudiciais e indesejáveis: é possível fazer uma modificação de mensagens que eventualmente tenham sido capturadas no meio do caminho sem que isso seja descoberto pelo receptor final devido à linearidade da função detectora de erros, e além disso, pelo fato de a função não possuir uma chave, é também possível descobrir uma seqüência secreta RC4 e de posse desta, ser autenticado na rede e introduzir mensagens clandestinas nesta.

Primeiras soluções propostas

Tendo-se em vista todas essas fraquezas do protocolo, algumas possíveis soluções foram propostas a fim de contornar e por que não acabar com tais fraquezas.

Uma das soluções que foram cogitadas foi a substituição da CRC-32 por uma função de hash MD5 ou SHA-1 por exemplo. No entanto, esta seria uma solução muito cara, além de tornar a execução do protocolo pelos atuais processadores muito lenta.

Uma outra solução discutida foi descartar os primeiros 256 bytes da saída do gerador de números pseudo-aleatórios utilizado na criação dos vetores de inicialização. Isso seria feito devido à alta correlação dos primeiros bits exalados pelo RC4 com a chave. Porém, essa solução mostrou-se também muito cara e para muitas aplicações, inviável de ser implementada.

Então, no final do ano de 2001, o pessoal dos laboratórios RSA sugeriu que para contornar as fraquezas do WEP fosse usada uma função de hash mais leve, que usasse uma chave temporária para criar chaves diferentes para cada pacote.

Na proposta, mostra-se que essa função de hash mais simples seria composta de duas fases distintas.

Na primeira fase teríamos como entrada a chave temporária TK e o endereço do transmissor TA. Ter o endereço de quem está transmitindo como parâmetro é muito vantajoso para evitar que seqüências RC4 sejam repetidas. Imagine, por exemplo, uma estação que só se comunica com o AP. A informação trocada entre eles utiliza a mesma chave temporária TK e isso aumenta as chances da seqüência se repetir, bastaria que o mesmo vetor de inicialização fosse utilizado para isso ocorrer.

No entanto agora, juntamente com a chave temporária, a estação utilizará seu endereço para gerar suas seqüências RC4 e da mesma forma, o AP utilizará seu próprio endereço para gerar suas seqüências. Dessa forma, evita-se a repetição de

seqüências dificultando dessa forma alguns ataques.

Na segunda fase proposta, a entrada seria a saída da primeira fase, e o vetor de inicia–lização. A saída dessa segunda fase seria então o que chamaram de PPK, ou seja, uma chave de 128 bits, diferente para cada pacote.

Apesar desta não ter sido a solução "final", embora a solução final não exista, pois sempre há atualizações para serem feitas e novos conceitos para serem implementados, os conceitos de chave temporária e chave por pacote foram importantes e serviram de base para a criação de um protocolo intermediário; eu diria que chega a ser um "protocolo paliativo" criado especialmente para aqueles que usam redes sem fio e prezam tanto a segurança que não podem esperar pelo WPA2 que chegará ao mercado provavelmente ainda neste ano. É sobre esse protocolo de caráter emergencial que falaremos a seguir.

WPA, um WEP melhorado

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA, que apesar de não ser um padrão IEEE 802.11 ainda, é baseado neste padrão e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente:

- Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado.

- Migrar para WPA requer somente atualização de software.

- WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do WPA sobre o WEP

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso à rede.

Referências

1 - R. Rivest, "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4", RSA Data Security, Inc., http://www.rsasecurity.com/rsalabs/technotes/wep.html

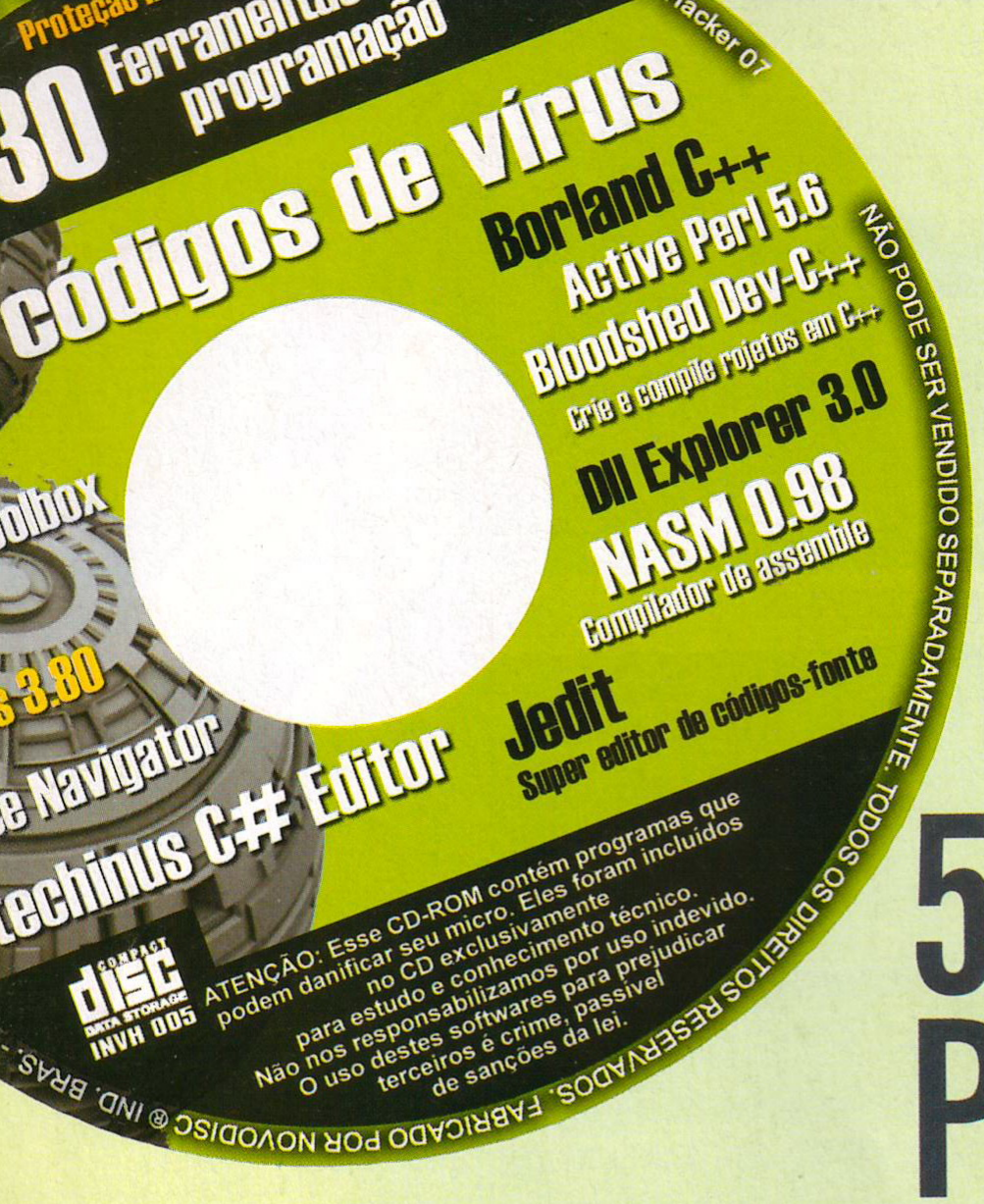
2 - F. Verissimo, "Em defesa de Rivest", Lockabit, Dezembro: www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=55

3 - R. Housley and D. Whiting, "Temporal Key Hash", IEEE techical Report: IEEE 802.11-01/550r3
http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-550.zip

4 – Borisov,N., Goldberg, I., and Wagner, D. "Intercepting Mobile Communications: Tha Insecurity of 802.11"

5 – Fluhrer, S., Mantin, I., and Shamir, A. "Weakness in the Key Scheduling Algorithm of RC4"

Isabela Chaves Santos é aluna do Departamento de Engenharia Eletrônica e de Computação, da Escola Politécnica da UFRJ, e membro do Grupo de Atuação em Redes sem Fio (GARF), do Laboratório de Redes de Alta Velocidade (RAVEL).



programas do CD-ROM

Estes são os destaques do seu CD-Rom:

500 VÍRUS PARA SEU ESTUDO E UM INCRÍVEL KIT DE FERRAMENTAS PARA PROGRAMAÇÃO

ATENÇÃO:

O uso indevido ou sem conhecimento técnico dos programas contidos neste CD-ROM podem danificar seu micro.

Em caso de dúvidas não execute!

Eles foram incluídos no CD exclusivamente para estudo e conhecimento técnico. Não nos responsabilizamos por mau uso. O uso destes softwares ou arquivos, para prejudicar terceiros é crime, passível de sanções da lei. Limitações de alguns programas shereware ou trial são eterminadas pelos desenvolvedores, não sendo responsa–bilidade dos editores.

Neste CD-Rom você vai encontrar mais de:

50 Ferramentas, programas para Windows e Linux

Primeiro você compra sua revista. Depois, curte o filhão à vontade.

WWW.ESCALA.COM.BR

WWW.ESCALA.COM.BR. Este é o endereço da nossa revistaria virtual, totalmente disponível, pra você! Muita informação, entretenimento, rapidez, conforto, segurança, além de muita variedade, é o que o site da Editora Escala reserva para você fazer suas compras com muito mais tranqüilidade.

ENTRE E FIQUE BEM À VONTADE, A REVISTARIA É SUA!

WWW.ESCALA.COM.BR

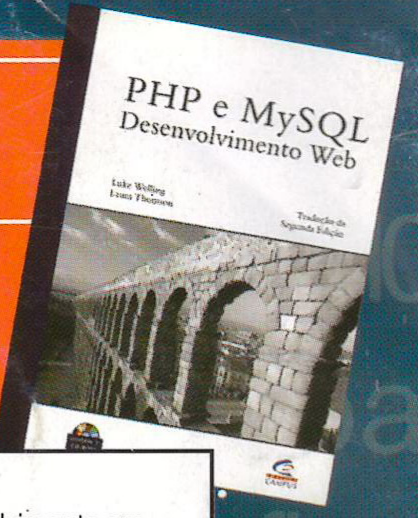
Compre com VISA

EDITORA escala

+ de 50 softwares

Kit de ferramentas para Programação

Editora Campus
677 Páginas + CD



Na edição número oito sai o resultado da promoção: ganhe um livro PHP MySQL.
Mande um e-mail para editorialph@yahoo.com.br com sugestões de artigos

Vírus
Mais de mil códigos das mais conhecidas pragas virtuais

Redes - Snifer

Effe Tech HTTP
Sniffer e analisador de pacotes - Shareware
Galaxy Spy
Monitora e grava todas as atividades entre seu PC e a rede que você acessa - Trial
ICMP datagram sniffer v1.0
Programa para DOS
NetWorkActive
Rastreia e analisa pacotes que circulam via TCP/IP - Requer Windows 2000\XP
OneWay Redes
Permite analisar e até salvar arquivos
Packet Sniffer
Sniffer de pacotes para Windows NT/2000/XP
Promisc Redes Sniffer
Checa se o adaptador de rede do Winindows NT /2000 está operando de modo promíscuo
SpyNet
Um ótimo network sniffer - Requer Internet Explorer 4.0 ou superior
Web Packet Sniffer
Script desenvolvido em Perl para analisar o tráfego de pacotes

Programação

emu8086 2.04
Software que combina múltiplas funções em um só programa. Entre as funções estão: avançado editor de código assembly, emulador com debugger, disassembler etc.- Requer VB Run Time - Sharewar
Absolute Telnet 1.84
Cliente de Telnet e SSH com opções de segurança avançada.- Sharewar
Active Perl 5.6
Interpretador Perl para servidores com plataforma Windows. Com esta ferramenta de desenvolvimento, você poderá executar scripts com a extensão PL em qualquer servidor Windows, facilitando a vida dos não-adeptos do Unix/ Linux. - Requer Windows Installer - Freeware

Antechinus C# Editor 4.2
Editor de código C# para compilar e criar aplicações.- Requer Microsoft's .NET Framework - Sharewar
Applyit!
Permite criar formulários e aplicativos em C++ para serem impressos. - Sharewar
Arisesoft Winsyntax 2.0
Editor de código PHP gratuito. - Freeware
Asp Compiler 1.0
Compile páginas e scripts em ASP. - Algumas funções desabilitadas - Demo
AutoEXE 1.0
Crie seus próprios arquivos auto-executáveis.
BinEdit 1.0
Abra e edite qualquer programa auto-executável com este editor de arquivos binários. - Freeware
Bloodshed Dev-C++ 4.0
Crie e compile projetos em C++. Esta plataforma de desenvolvimento possui diversos recursos que facilitam a vida do programador como as ferramentas para compilar e executar projetos. - Algumas opções desabilitadas - Sharewar
Borland C++ Compiler 5.5
Excelente compilador de C++ da Inprise. Esta poderosa ferramenta de desenvolvimento pode ser usada para a criação de aplicações para Internet, desktop, client-server, sistemas distribuídos e muito mais. E o melhor de tudo é que este software é gratuito - Requer registro no site da Borland - Freeware
Borland C++ 3.1
O Borland C é um programa que permite trabalhar com a linguagem de programação C.
CobolScript Version 2.10
Tem a sintaxe parecida com a linguagem de programação COBOL e é ideal para conversão de dados e para a criação de scripts.
Codewhiz 1.7
Programa especial para editar códigos-fonte. - Sharewar
Deface Tool v1.0
Ferramenta que ajuda a deixar sua marca no site invadido.
Developer's JavaScript Editor 0.6
Para visualizar e editar JavaScripts. - Open Source
Dll Explorer 3.0
Visualize todos os processos que estão sendo executados em seu computador. Além disso é possível examinar arquivos DLL, EXE e outros. – Sharewar
Euphoria 2.3
Conheça essa nova linguagem de programação. Linguagem de programação simples e flexível voltada especialmente para o desenvolvimento de aplicações 32-bits Dos e 32-bits Windows. - Sharewar
GCC (Linux)
Compilador para programar exploits em C (em várias versões) Open Source
Jedit
Super editor de códigos-fonte, que suporta mais de 70 linguagens. - Opensource
Kopi Compiler Suite 2.1A (Linux)
KOPI é um compilador GPL de Java, ferramenta muito poderosa para o desenvolvimento de aplicações das bases de dados que empregam Java, o JDBC e o JFC/Swing. - Opensource
Digital Mars C/C++ Compiler 8.31
Compilador para linguagem C/C++
Mihov Code View 1.1
Visualizador de códigos-fonte e documentos de texto e HTML. - Freeware
Miracle C Compiler 3.2
Ambiente de desenvolvimento integrado padrão ANSI e compilador C. Software é capaz de trabalhar com vários projetos ao mesmo tempo, possui sintaxe original da linguagem C, bibliotecas de funções e programas-exemplos. - Sharewar - Requer Windows Installer
NASM 0.98
Compilador de assembly para microprocessadores 80x86. Programa utilizado para o desenvolvimento das plataformas Windows9X, Windows NT, MS-DOS, Linux, Alpha, entre outros. - Freeware
NoteTab Light 4.9
Para escrever seus códigos-fonte de um jeito simples e rápido. - Não definida
Perl Dev Kit 4.1.2 (Linux)
Ferramentas para desenvolver scripts e exploits em Perl. - Requer Active Perl
PHP Expert Editor 2.5
Para criar, editar e compilar PHP scripts. – Sharewar
PHP Triad 2.11
Ambiente integrado para desenvolvimento em PHP. Neste programa estão incluídos o servidor MySql, Apache e o PHP. Todos estes componentes são OpenSource, ou seja, livres e gratuitos
PyChecker
Encontra erros de programação em programas desenvolvidos em Python. - Não definida
Assembly-Language Toolbox
Ferramentas de Assembly para Qbasic. - Sharewar
Resource Hacker 3.4
Utilitário para visualizar, adicionar, deletar e extrair recursos em aplicações Windows de 32 bits. - Freeware
SecureCRT 4.0
Emulador de terminais SSH e Telnet. SecureCRT combina as potencialidades de login´s e transferência de dados de SSH (Secure Shell) com a confiabilidade e configurabilidade de um Windows terminal emulator. - Shareware
Create Install
Crie de arquivos de setup de maneira rápida e fácil. - Trial
Source Navigator
Ferramenta de análise de códigos-fonte
X Language 0.5
Linguagem de programação com intérprete, debugger e compilador JIT. - Opensource
XVI32 2.21
Editor hexadecimal para engenharia reversa de softwares - Freeware
Zeus for Windows 3.80
Ambiente integrado de desenvolvimento com suporte às linguagens C/C++, Java e Perl destinado a programadores profissionais. Possui compilador que roda em background, funções undo/redo que tornam mais fácil e produtiva à elaboração do seu projeto.

Souce Code

6XS
Código-fonte do Secure Internet Communication Suíte.

Crack Whore 2.2
Fonte do programa feito para testar a segurança de sites.

GnuPG
Código-fonte do GNU Privacy Guard. 1,85 MB

Java Telnet Applet 2.0
Programa de Telnet para acesso remoto

Pattern Finder
Programa em java para buscar vírus

Ultimate
Código-fonte de um Bot programado em V Basic

Zodiac
Versão em desenvolvimento de um programa de análise de protocolo DNS.

"Programa" da matéria

Engenharia reversa do Mydoom
Script exclusivo, completo do vírus Mydoom.