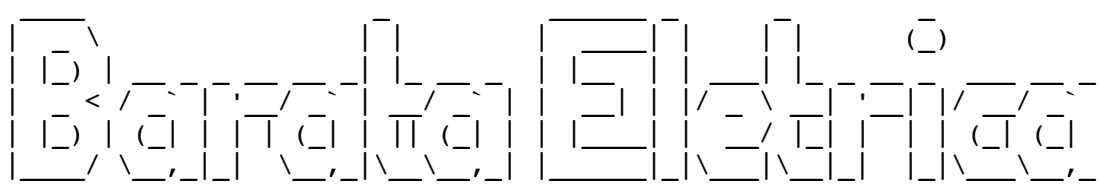


BARATA ELETRICA, numero 12
Sao Paulo, 20 de agosto, 1996

Creditos:

Este jornal foi escrito por Derneval R. R. da Cunha
(wu100@fim.uni-erlangen.de - http://www.geocities.com/SiliconValley/5620)
(rodrigde@usp.br, derne@geocities.com)

Para contatos (mas nao para receber o e-zine) escrevam para:

rodrigde@spider.usp.br
derne@geocities.com
wu100@fim.uni-erlangen.de

Correio comum:
(Estou dando preferencia, ja' que minhas contas vao e vem sendo "congeladas")

Caixa Postal 4502
CEP 01061-970
Sao Paulo - SP
BRAZIL

Numeros anteriores (ate' o numero 10):

ftp://ftp.eff.org/pub/Publications/CuD/Barata_Eletrica
gopher://gopher.eff.org/11/Publications/CuD/Barata_Eletrica
http://www.eff.org/pub/Publications/CuD/Barata_Eletrica

ou ftp://etext.archive.umich.edu/pub/Zines/BerataElectrica
gopher://gopher.etext.org/00/Zines/BerataElectrica
(contem ate' o numero 8 e e' assim mesmo que se escreve, erro deles)

ATENCAO - ATENCAO - ATENCAO
Web Page do Fanzine Barata Eletrica:
http://www.geocities.com/SiliconValley/5620
Contem arquivos interessantes.
ATENCAO - ATENCAO - ATENCAO

NO BRASIL:

http://www.inf.ufsc.br/ufsc/cultura/barata.html
http://www.di.ufpe.br/~wjqs
http://www.telecom.uff.br/~buick/fim.html
http://tubarao.lsee.fee.unicamp.br/personal/barata.html
ftp://ftp.ufba.br/pub/barata_eletrica

(Normalmente, sao os primeiros a receber o zine)

MIRRORS - da Electronic Frontier Foundation onde se pode achar o BE
/pub/Publications/CuD.

  UNITED STATES:
etext.archive.umich.edu in /pub/CuD/Barata_Eletrica
ftp.eff.org in /pub/Publications/CuD/Barata_Eletrica
aql.gatech.edu in /pub/eff/cud/Barata_Eletrica
world.std.com in /src/wuarchive/doc/EFF/Publications/CuD/Barata_Eletrica
uceng.uc.edu in /pub/wuarchive/doc/EFF/Publications/CuD/Barata_Eletrica
wuarchive.wustl.edu in /doc/EFF/Publications/CuD/Barata_Eletrica
  EUROPE:
nic.funet.fi in /pub/doc/cud/Barata_Eletrica
                  (Finland)
(or /mirror/ftp.eff.org/pub/Publications/CuD/Barata_Eletrica)
ftp.warwick.ac.uk in /pub/cud/Barata_Eletrica (United Kingdom)
  JAPAN:
 ftp.glocom.ac.jp in /mirror/ftp.eff.org/Publications/CuD/Barata_Eletrica
 www.rcac.tdi.co.jp in /pub/mirror/CuD/Barata_Eletrica

OBS: Para quem nao esta' acostumado com arquivos de extensao .gz:
Na hora de fazer o ftp, digite binary + enter, depois digite
o nome do arquivo sem a extensao .gz
Existe um descompactador no ftp.unicamp.br, oak.oakland.edu ou em
qualquer mirror da Simtel, no subdiretorio:

/SimTel/msdos/compress/gzip124.zip to expand it before you can use it.
Uma vez descompactado o arquivo GZIP.EXE, a sintaxe seria:
                          "A>gzip -d arquivo.gz

No caso, voce teria que trazer os arquivos be.??.gz para o
ambiente DOS com o nome alterado para algo parecido com be??.gz,
para isso funcionar.

==========

ULTIMO RECURSO, para quem nao conseguir acessar a Internet de forma direta,
mande carta (nao exagere, o pessoal e' gente fina, mas nao e' escravo, nao
esquecam aqueles encantamentos como "please" , "por favor" e "obrigado"):

fb2net@netville.com.br
hoffmeister@conex.com.br
drren@conex.com.br
wjqs@di.ufpe.br
aessilva@carpa.ciagri.usp.br

dms@embratel.net.br
clevers@music.pucrs.br
rgurgel@eabdf.br
invergra@turing.ncc.ufrn.br

CREDITOS II :
Sem palavras para agradecer ao pessoal que se ofereceu para ajudar na distribuicao do E-zine, como os voluntarios acima citados, e outros, como o sluz@ufba.br (Sergio do ftp.ufba.br), e o delucca do www.inf.ufsc.br Igualmente para todos os que me fazem o favor de ajudar a divulgar o Barata em todas as BBSes pelo Brasil afora.

OBSERVACAO: Alguns mails colocados eu coloquei sem o username (praticamente a maioria) por levar em conta que nem todo mundo quer passar por colaborador do BE. Aqueles que quiserem assumir a carta, mandem um mail para mim e numa proxima edicao eu coloco.

INTRODUCAO:

O mes de julho foi uma caca. Nos mesmos dias em que estava colocando o BE11 para distribuicao tava planejando sair a caca de um novo emprego. Stress de final de semestre, caiu um monte de coisa tudo junto, a greve da USP terminou coincidindo todos os meus problemas: faculdade, habitacao e pequenas diferencas com o meu superior imediato. Ia criar mais um problema, se a coisa tivesse ido adiante: em que eu ia trabalhar, se saisse de onde estou... de um lado, a experiencia com informatica, do outro, a experiencia com o primeiro fanzine eletronico brasileiro (e acredito, o mais difundido e lido). Como arrumar 2000,00 Reais mensais de forma honesta? Ou apenas o suficiente p. se sobreviver numa cidade mais cara que N.York? No proximo numero, espero ter alguma resposta para essa pergunta.

O pior e' saber que uma revista inominavel publicou o meu nome num artigo. Oba! So' q. para ilustrar um exercicio de uso do EUDORA. O cara guardou correspondencia minha do ano passado (eu tambem guardo as mais importantes) para ilustrar uma materia. Quando meu artigo saiu na revista, so' quis meu pseudonimo, agora inventa um jeito de usar meu nome.. fosse outra revista, tava bem menos chateado. Fico ate' com medo de responder cartas, corto o papo o mais rapido possivel. Ou e' alguem que conheco fora do ciberespaco ou nada feito. Better safe than sorry. Como e' que vou saber q. o cara q. ta' me mandando cartas e' fulano e nao outro que pegou a conta emprestada? Pelo cheiro? Ai' criei um guia do q. acho que a netiqueta deveria ser. E nao parei ai'. Fiz um artigo (q. acabou ficando tao bom q. guardei p. meu livro e fiz outro menor) sobre passos basicos para usar o PGP. Sim, porque agora e' lei. Seu email pode ser vasculhado. Leitor do Barata Eletrica nao tem desculpa alguma p. nao me mandar correspondencia nao encriptada. Simplifiquei o maximo possivel. E' so' nao ter medo de errar. Se errar, leia a documentacao, ja' ta' traduzida pro portugues.

Recebi uma carta quase incrivel de duas pessoas querendo mover uma campanha p. ajudar o Mitnick. Ainda bem q. nao sou so' eu que acredita no excesso de rigor da prisao do cara. Tinha q. publicar. Amanha, pode ser eu. Parece paranoia.. ta' bom. Em 1978, teve um cara q. achava q. ir ao DOI-CODI prestar depoimento era algo sem perigo. Vladimir Herzog. Se nos EUA, fazem aquilo com o Mitnick, aqui no Brasil nao posso deixar de ficar preocupado. Como dizia a cobra pro elefante: "se liga, meu, que e' estacao de caca as cobras" o elefante: "e dai', sou elefante" a cobra: "prova pra eles". Eu nao sei quem sao eles. Mas acredito em ficar ligado.

INTRODUCAO
NET DICAS E ETIQUETAS PARA FUCADORES

NET-DICAS E ETIQUETA PARA FUCADORES

Uma coisa que reclamam pra caramba nestes dias e' que tem gente demais entrando na Internet. Tudo bem, e' assim que tem que ser mesmo. O ideal e' o mundo inteiro estar conectado. Comunicacao e' um direito, assim como a respiracao, do meu ponto de vista. Mas para um dinossauro (giria p. alguem que foi quase pioneira na Internet - acho q. cheguei a esse ponto) como eu, e' dose ver que a mocada nao le po nenhuma sobre como se comportar na rede. Muitos poucos leem o "Zen e a arte da Usenet" ou porque nao sabem ingles, porque nao sabem da existencia do livro, nao sabem da traducao, nao sabem imprimir a dita (ta' em Postscript), ou porque tiveram preguica de chegar no capitulo referente a netiqueta. Por ultimo, tem gente tao ligadaca na rede que nao sabe que tem um "caminho das pedras" para conseguir a ajuda das pessoas. E pagar o equivalente a dois meses de conexao para ler algum daqueles livros sobre a rede que estao lancando todo dia por ai', meu, nem eu faria isso. Um absurdo o que se paga para nao aprender nada.

Pra esclarecer:

Vou colocar um apanhado de dicas que e' mais ou menos o que utilizo. Nao aconselho ninguem a seguir esses lances, porque provavelmente, grupos diferentes usarao regras diferentes. Comecando com o numero 1. Para evitar a ideia de que uma dica e' mais importante do que a outra, random(N) significa numero aleatorio.

1) Nunca imagine que voce esta' falando com uma maquina. A pessoa do outro lado e' gente como voce. Por incrivel que pareca, com sentimentos.

Random(N) Ha arquivos, a grande maioria em ingles, armazenados na rede e chamados de FAQ (Frequent Answered Questions) ou Perguntas Mais Respondidas. Isso significa que sao perguntas que todo iniciante faz, quando entra em alguma lista. No caso da Internet, existem varios textos introdutorios, que ajudam. Recomendo o Big Dummy Guide, disponivel no ftp.eff.org ou www.eff.org.

Random(N) Quando a pessoa usa o comando TALK, sente uma subita necessidade de experimentar aquela coisa de comunicacao via teclado. So' que o uso desse comando gera uma mensagem na tela de outra pessoa, que pode estar ocupada fazendo o download de um arquivo de 20 megabytes com a biografia falada do Julio Iglesias (ou um salvador de tela da Madonna, sei la'). O comando fica repetindo na tela e atrapalha a digitacao de cartas, por exemplo. O ideal e' deixar o TALK "ringar" (chamar a pessoa) umas tres vezes, cancelar, esperar e depois de um tempo, se nao houver resposta, tentar de novo, para em seguida desistir. Tem gente que deixa a coisa tocando direto, ate' a pessoa do outro lado resolver atender. E' a mesma sensacao de sair do banho p. atender o telefone.

Random(N) Usando o IRC, nao pega muito mal ficar so' escutando (ou lendo) o papo que ta' rolando, antes de falar (escrever) qualquer coisa. Parece

obvio, mas varios dos que entram estao tao "excitados" de conseguir que nao se dao conta do fato de que estao pegando o bonde andando.

Random(N) Novamente, ao usar o IRC, e' legal usar um nickname ou apelido. De preferencia um proprio e nao copiado. E' quase como uma identidade da pessoa. Algumas vezes e' ate' pista p. identificar o jeito da pessoa. Se bem que ja' ouvi falar de gente que usa nicknames como "metobem" so' para nao ser chamada p. bater papo. Ou mesmo provocar.

Random(N) Tanto no e-mail, quanto nas listas, quanto no IRC: Nao e' porque voce esta' usando um computador p. conversar que voce pode falar o que quiser tanto sobre voce como sobre o governo, como sobre o mundo. Se liga. Houve um cara que foi processado, anos atras porque falou que um livro sobre o DOS 6.0 na verdade era para o DOS 5.0, com alguns acrescimos so' p. enganar. Foi processado por perdas e danos. Perdeu ou ganhou o processo? So' o tempo que gastou com advogado ja' foi uma perda. Sobre falar sobre voce, tudo depende da plateia e da forma que voce escreve. Imagine virar fofoca no lugar onde voce menos espera. Voce realmente sabe quem esta' ouvindo? Consegue se controlar para nao transformar o ouvido alheio em pinico? Teve o cuidado de proteger seu anonimato antes de entrar no papo?

Random(N) Voce gastou talvez 2.900 US$ num computador multimidia para falar (escrever) porcaria sobre gente que se conecta na Internet com um XT ou um 286? Po^... se voce levar em consideracao o fato de que artigos desse fanzine eletronico ja' foram escritos numa agenda eletronica, para nao falar na maioria, que foi escrita num PC-Xt com dois drives 5 1/4 DD, 640 kbytes RAM, sem disco rigido e monitor CGA mono, 8 mhz. Uma questao de sanidade. Mental e fisica. E', podia ser num Pentium, so' q. quero dormir, quando chego em casa. De vez em quando e' bom. Mas voltando a questao da crenca religiosa, tem aqueles que rezam pelo Mac, tem uns firmes que o bom e' o MSX, outros pelo Apple. Nao discuto essas coisas sem uma cerveja do lado. Se te pintar a vontade de abrir uma discussao, pergunte algo tipo: "quais as vantagens de se usar um ZX-80 nos dias de hoje?" ao inves de "meu, larga a mamadeira, economiza e compra um Pentium". Eu ia esperar um Pentium p. poder editar o Barata Eletrica? To nem ai'. Melhor parar o papo.

Random(N) Existe muito papo sobre enviar ou nao o seu numero do cartao de credito via e-mail, na rede Internet. E', de um lado, as chances de voce ter o dito copiado por um garcom num restaurante, na hora de pedir a conta ou ser assaltado sao um pouco maiores. Por enquanto. No futuro, quem sabe? O email pode passar por uns quinze sites diferentes antes de atingir o destinatario. Believe me. Basta um site ter sua seguranca compromissada. Suponha que isso aconteca no Natal e .. bom, tem gente que acredita em poder do pensamento positivo, em consorcio, em promessa de politico, impressionante, ne'?

Random(N) Um lance chato sao as .signatures, aqueles finais de e-mail cheios de informacao sobre o cara que respondeu sua pergunta com um "OK". Tudo bem 5 ou 6 linhas. O ideal e' no maximo 4, principalmente quando e' "macaco velho" da Internet. Novato e' que faz uns desenhos enormes, para colocar do lado da assinatura. Tem gente que seta o software de email p. apagar fulanos q. fazem isso em listas de discussao, dentro e fora da Usenet. Alias, a impressao e' que quanto maior a signature, menos a pessoa tem o que contribuir. E isso tambem chama uma atencao maior, quando o "super-visual" escreve bobagem. E' o tipo de coisa que e' bom fazer so' p. descobrir o quanto e' ruim. Claro que a gente presta mais atencao na signature dos outros do que na nossa.

Random(N) Namoro eletronico. Putz, ja' se escreveu tanto sobre isso.. E' preciso lembrar o obvio. Papai Noel nao existe. E' duro falar isso, mas tem

gente que nao aprende. Tem gente ruim por ai'. E gente boa, tambem. Voce pode conhecer uma pessoa super-legal, compreensiva, alto astral, papo franco e aberto, coracao disposto a mil e uma coisas gostosas.. e pode tambem encontrar um sacana que ta' usando o email da mae (ou pai ou irmao) e que ta' tirando sarro da sua cara. Se voce ta' namorando alguem, tem varios testes p. sacar quando e' mulher. Nao adianta, se voce nao quer acreditar. Ja' vi fucador de micro tomar choque so' porque babou demais num teclado quando recebeu carta de mulher (ta' bom, nao houve choque eletrico). E' preciso pensar q. por enquanto, a grande maioria na rede e' homem. Uma dica: se ela fez muito misterio, desencana... ou marca um encontro ao vivo.

Random(N) Ao enviar uma carta, de um tempo p. as respostas. Se a pessoa nao responder imediatamente, nao fique desesperado pensando o q. e' que voce fez de errado. Algumas vezes, o servidor caiu, a pessoa ficou doente, chegou o marido, o gato pisou no teclado, etc.. as vezes, e' falta de vontade mesmo de responder. Fazer o que?

Random(N) Pedir numa lista de discussao, p. mandarem o COREL DRAW ou o PAGEMAKER 6.0 e' coisa seria. Fimose cerebral. Pirataria de Software e' crime. Outro crime e' pensar que se pode mandar megabytes e megabytes via e-mail como se fosse uma carta de "oi, tudo bem". Outra idiotice e' pensar que um idiota capaz de pedir tal coisa por e-mail seja capaz de fazer o dito funcionar no micro dele (as vezes existem protecoes que impedem isso). Por essas e outras, se a cabeca servisse para alguma coisa, a desse tipo de gente certeza tava no lixo. Existem as listas de discussao de Warez. Mas quem frequenta usa truques p. evitar deteccao, sabe q. o software q. pinta, dividido em partes de 40 kbytes (p. facilitar o download) pode estar virotico e ... em suma, e' gente q. sabe o que esta' fazendo. O unico software que e' legal enviar por e-mail e' principalmente shareware ou dominio publico.

Random(N) Se for enviar arquivos volumosos p. alguem, manda primeiro um aviso. Prinicipalmente quando o negocio for arquivos .WAV ou .GIF. Combina, do contrario pode ferrar com o limite de email da pessoa.

Random(N) Quando for conversar coisas "incriminantes", do tipo que nao e' crime conversar, mas fora de um contexto pode parecer conspiracao para um fazer sacanagem, ve se usa uma linguagem de duplo sentido ou melhor, usa um talker (ver edicoes anteriores). Nao combine sacanagem por e-mail. Lembre-se do "Big Brother". Existe software p. alertar que fulano usa muitas vezes a frase "craquear o sistema" no email. Na verdade ate' um comando do DOS, executado a partir de um arquivo .BAT pode checar em poucos segundos um arquivo de email. Um comando do UNIX, o grep, tambem pode fazer isso. Pensa nisso. Voce acredita em integridade e justica por parte do seu Sysop? E em duende, acredita? Sabia que as plantas tambem falam? Entao se liga. Ha' coisas relacionadas a computacao que nao sao crime. Cortar o seu acesso a internet pode ser uma delas. Toma cuidado.

Random(N) Na Internet ninguem pode ouvir voce chorar. Mas existe uma convencao p. quando a pessoa esta' GRITANDO. E' O USO DE TECLAS MAIUSCULAS, ENTENDEU?

Random(N) NUNCA USE CEDILHA NEM ACENTUACAO, SE NAO QUISER OUVIR PALAVRAO NOS REPLY. O uso de acentuacao e outras coisas q. seriam consideradas como "bom portugues" na verdade atrapalha a vida de um monte de gente. Se quiser acentuar crase, use aa (p. exemplo). O Barata Eletrica tem um monte de exemplos de como fingir acentuacao. Repito: se quiser ser popular, nao use acento nem cedilha.

Random(N) Novamente, sobre dicas e macetes. Tome cuidado com gente que escreve umas dicas. Se voce nao tem o conhecimento necessario p. avaliar o que esta ou aquela dica faz, please nao faca uso dela. E' muito facil ocultar sob esta ou aquela sequencia de comandos uma instrucao p. mandar o conteudo do arquivo de senhas p. outra pessoa. Ou algo como "echo_y_|_format_c:" (Na teoria poderia formatar o disco rigido, sem pedir permissao p. usuario, mas na pratica, nao funciona).

Random(N) Nao entre nessa de ouvir boatos que estao rolando na rede. Volta e meia vem aquela estoria contando q. a acao de empresa tal vai subir, o dolar vai disparar no black (jura?), a China vai tornar o homossexualismo obrigatorio p. conter a natalidade, que a Sharon Stone e' a re-encarnacao da Virgem Maria, etc So' porque a coisa esta' na Rede Internet, nao significa que e' verdade.

Random(N) Virus GOOD TIMES. Nao existe. O que acontece e' que o medo de virus (todo mundo tem) cria uma avalanche de e-mails, todo mundo escrevendo p. a sua lista de discussao preferida avisando p. se precaver contra a mais nova ameaca na rede Internet. Esse e' o virus. O do medo. Ele lota seu email de cartas inuteis de gente pensando que vai te ajudar avisando que tem um virus capaz de deletar sua winchester, quando voce le um e-mail contaminado. Nao caia nessa.

Random(N) Tambem tem gente q. tenta fazer acreditar que se pode ganhar dinheiro facil atraves da Internet. Nao caia nessa. Coelhinho da Pascoa, Papai Noel, etc isso so' existe na imaginacao. E' duro, mas caia na real. Tem gente q. faz grana, mas e' trabalhando duro, nao por e-mail. Mesmo q. a coisa aconteca, pensa bem: sera' que e' mesmo verdade? Eu nao acredito em nenhuma forma "facil" de ganhar dinheiro com a Internet. Minha opiniao pessoal. Apesar que me falaram da existencia de "cassinos" na Web. Depois de assistir o filme "Cassino", vale a opiniao de Nelson Rodrigues "Burro nasce que nem grama". So' tem uma pessoa que ganha com esses esquemas e e' a que convence os idiotas a acreditarem nele.

Random(N) Procure sempre guias que te instruam. Provavelmente voce podera' sanar suas duvidas mandando carta para sysop@servidor.???.br ou root@servidor.???.br, mas o ideal e' cacar FAQs (Frequently Answered Questions) que vao conter todas as suas duvidas. Sao artigos escritos para novatos aprenderem os conceitos basicoa sem atrapalhar os veteranos. Ha' varios como http://www.fgv.rj.br/fgv/cpdoc/informa/guianet.htm

Random(N) Sobre amizades virtuais. Normalmente a coisa comeca em torno de um assunto especifico. A pessoa participa de um grupo de discussao, Iphone, IRC ou Talker (formas de bate-papos virtuais), etc.. a partir dai', por varias razoes, pinta a vontade de bate-papos individuais. O motivo porque o ser humano procura "contato humano" atraves do uso de computadores interligados pode ser a dificuldade de andar pelas ruas, o medo da rejeicao, a falta de tempo, o anonimato, a facilidade de uso da rede, etc, etc.. e' algo que vicia. Pode ser uma boa. Mas aconselho o dobro de precaucao. Quando se conversa via micro, mesmo com Iphone, nao se tem o fluxo-de-dados de uma conversa ao vivo. Esta, de acordo com os cientistas, tem um fluxo de dados q. alcanca 2000 sinais simultaneos (expressao no rosto, tom de voz, piscadelas, etc). Na internet, ninguem sabe se voce e' um cachorro usando o focinho p. teclar as palavras. E' muito facil mentir e ouvir mentiras. Evite falar qualquer coisa seria on-line. Tipo: voce tem certeza q. a pessoa q. esta' te lendo (ouvindo) no talker nao e' seu inimigo? Ja' aconteceu comigo.. o desgracado ate' me elogiou, antes de esticar o pescoco e descobrir que era eu no computador no fundo da sala.

O NOVO FRONT DA GUERRA ELETRONICA

Novembro, 1992 - Cerca de dois mil computadores ligados a rede ARPANET (que deu origem a Internet) estao imobilizados por um estranho programa-virus. O panico se instala, ja' que a unica saida para combater a infeccao e' desconectar as maquinas da rede. Tecnicos encarregados da manutencao nao conseguem nem "abrir" uma sessao p. enxergar que catzo esta' acontecendo. Analise do "invasor" revela que o codigo do programa esta' criptografado, para evitar que programadores descubram como combate-lo. Quando este virus, que foi apelidado de "Worm" ou minhoca, entra em atividade, comeca a se copiar para outros computadores, procurando por conexoes na rede. Achando uma maquina nova, copia-se para ela. Para passar por cima das senhas, usa nao um, mas varias tecnicas automaticas de craqueamento de contas internet, incluindo um dicionario de senhas simples e comuns, como nomes de mulher, times de futebol, etc e um programa de quebramento de senhas por forca bruta de algoritmo bastante sofisticado. As tecnicas de break-in, verdadeiros buracos no sistema operacional dos computadores atingidos eram de conhecimento mais ou menos difundido entre peritos de computacao. A unica funcao do codigo era a reproducao ou copia automatica. Se uma copia fosse apagada, outra surgiria para tomar o lugar e essa multidao lotaria a memoria de quase qualquer sistema multi-usuario conectado a rede. O autor desse codigo, Robert T. Morris, filho de um cientista do NSA, foi apontado como o autor da ameaca. Autor de um programa bastante famoso, conhecido como COREWAR, um jogo de computador (bastante difundido hoje em dia com FAQs e listas de discussao) onde programadores disputam o controle de uma CPU atraves do uso de programas que lutam entre si ate' a morte, Morris cometeu uma serie de erros ao projetar o Virus. Nao acrescentou uma rotina que impediria um alastramento desenfreado. Essa infeccao generalizada teve que ser contida com base em chamadas telefonicas, ja' que os computadores atingidos estavam fora da rede.

Esse foi um dos primeiros casos de crime por computador a chamar a atencao da midia (e uma das primeiras condenacoes, mas e' outra historia). Mostrou tambem a vulnerabilidade da recem construida rede Arpanet, lancou na midia o termo virus de computador e .. inaugurou uma nova possibilidade de guerra: o front da guerra eletronica. Nao se trata de mera fantasia. O sistema telefonico de um pais e' um computador, para se ter uma ideia. Em 15/01/1990, foi exatamente isso o que aconteceu com os telefones americanos. Em pleno feriado da morte de Martin Luther King, todos os sistemas de DDD dos EUA pararam de funcionar. Culpa de um defeito ou "bug" que se alastrou de sistema em sistema de telefonia. 60 milhoes de ligacoes telefonicas deixaram de ser completadas, durante as nove horas que durou o esforco para consertar a coisa. A primeira coisa em que todo mundo pensou e' que um moleque (e', uma crianca) com seu micrinho tivesse detonado a coisa. Mais tarde se chegou a conclusao de que era mesmo um erro de programacao (apesar de uns idiotas assumirem a autoria da coisa).

A sociedade atual, como a conhecemos, existe apoiada nos computadores. Computadores fazem o controle dos sinais de transito, a contabilidade das contas de luz, o pagamento de funcionarios, o planejamento de recursos, a transferencia de fundos entre bancos, a transferencia de fundos entre bancos e a nao menos transferencia de fundos entre bancos. Cada pessoa, que vai numa agencia "Banco 24 horas" para tirar uma grana, realizou uma conexao via protocolo X-25 (parece que agora vai mudar para frame-relay) com um computador central que esta' conectado com a agencia onde esta' a conta bancaria. A maioria das pessoas ja' conhece o termo "a agencia esta' fora do ar". E' uma conexao feita dentro da RENPAC, a rede nacional de pacotes, da Embratel.

Claro que com o fim da guerra fria, as chances de uma guerra mundial estao bastante diminuidas. Por um outro lado, a exploracao desse novo front

de ataque ja' e' tema de exploracao de livros como o TERMINAL COMPROMISE (ftp://mrcnext.cso.uiuc.edu/etext/etext95/termc10.zip) do Winn Schwartau e INFORMATION WARFARE. Talvez comentando o livro se possa entender a seguinte noticia:

> E D U P A G E 21 de julho 1996
> OFICIAIS DOS EUA EMITEM AVISO SOBRE O "ELECTRONIC PEARL HARBOR"
>
> Jamie Gorelick, procuradora geral dos EUA, disse no subcomite do Senado na semana passada que a possibilidade de "um Pearl Harbor eletronico" e' um perigo real para os EUA. Ela observou em seu testemunho que a infraestrutura de informacoes dos EUA e' uma rede publica/privada hibrida e avisou que ataques eletronicos "podem desabilitar ou romper adisponibilidade de servicos tao prontamente quanto - se nao ainda mais rapido - do que uma bomba bem instalada". Em 15 de julho, a Administracao Clinton formou uma Comissao de Presidente sobre a Protecao da Infra-estrutura Critica, com o proposito de identificar a natureza das ameacas a infra-estrutura norte-americana, tanto eletronica quanto fisica e de trabalhar com o setor privado no sentido de estabelecer uma estrategia para a protecao dessa infra-estrutura. Em uma audiencia recente, membros do sub-comite foram informados que a cada ano, ocorrem 250.000 intrusoes aos sistemas de computacao do Departamento de Defesa, sendo a taxa de sucesso da ordem de 65%.
>
> BNA Daily Report for Executives 17 jul 96 A22

Incrivel, ne'?

Mas nao e' so' num ou noutro jornal ou revista que os EUA estao se preparando. Hollywood ja' comeca a preparar a opiniao publica, haja visto o ID4, vulgo "4 de Julho", o filme sobre invasao extra-terrestre. Dava p. fazer um livro so' com as imprecisoes do filme (ideal como diversao). Mas nas entrelinhas, tava la' o futuro tipo de guerra. Um virus de computador colocado na nave-mae dos alienigenas (pra quem nao sabe, alien e' tambem sinonimo de estrangeiro em situacao ilegal), que permite o abaixamento das defesas e a vitoria final. Porem existem outras obras.

O Terminal Compromise e' um thriller. Daqueles que emanam uma afirmacao do tipo "nao li nada do Proust p. escrever isso". Mas e' uma obra de arte e merece ser lido (afinal de contas, ta' disponivel gratuitamente na rede). Os viloes sao parte frutos de situacoes de conflito nas quais os EUA se envolveu, como a guerra do Golfo, e comandados e financiados por um japones que faz o "Kaiser Soza" (filme "Os suspeitos") parecer apenas um "turquinho safado".

Toda guerra tem um motivo. No caso, a vinganca pelo bombardeio de Hiroxima, na 2a guerra mundial. Um sobrevivente, que se torna depois um rico e poderoso super-empresario, decide cobrar a coisa. O "general" dessa guerra e' um genio matematico recem-saido do NSA, agencia de inteligencia americana da qual nutre enorme ressentimento. O exercito, parte constituido por grupos terroristas islamicos, parte recrutado entre crackers e fabricantes de virus, parte constituido por escroques e malandros. Os terroristas ficam com tarefas como assassinatos, ameacas, espionagem atraves de sistemas TEMPEST e colocacao de bombas de efeito magnetico. O TEMPEST e' o maior risco atual no que se refere a invasao de privacidade, "enxergar" a emanacao da radiacao de uma tela de computador ate' a distancia de mais ou menos 1 quilometro de distancia. Existe. E' como ter sujeito olhando por cima do seu ombro a mais de um quarteirao de distancia tudo o q. aparece na tela do seu micro. So' imagina.. Sao usados monitores do tipo p. espionar industriais (no livro) com o fim de chantagem, para confundir o FBI, alem de facilitar break-ins em bancos de dados (no livro).

Os terroristas tambem plantam aqui e ali algumas bombas de efeito magnetico, capazes d apagar todos os dados armazenados em computadores meio perto da area de detonacao. Em instituicoes financeiras ... iam causar um estrago. Como saber quem depositou quanto, se os back-ups forem apagados?

Os crackers e hackers aparecem no seguinte esquema: uma companhia fabricante do software que abastece a maioria dos computadores americanos (donde se entende porque re-inventar uma historia da computacao atual) na verdade vende o software com um virus embutido, com data para funcionar a partir de uma data X. E isso nao e' tudo. A maior BBS do pais, responsavel pela divulgacao de software shareware e freeware na verdade infecta todos os seus programas com outros tipos de virus, tambem com data de ativacao no mesmo dia X. Durante o livro, se descobre que todas essas empresas foram compradas por gente controlada pelo empresario japones. Quem descobre isso? Um jornalista, que e' contactado por um hacker que nao gostou da materia e que resolve colocar o dito a par do que e' etica hacker. Isso porque "thriller" sempre trabalha no esquema de um mocinho que nao manja nada de nada, mas no trabalho de entender tudo, recebe as explicacoes que o leitor precisa, para acreditar na historia. E e' uma senhora viagem no "computer underground", completando o livro Hacker Crackdown, do Bruce Sterling. Os hackers ajudam a salvar a patria, revelando como tirar os virus e como solucionar os problemas de software causados pelo "exercito" inimigo. A imprensa faz um otimo trabalho de divulgacao desse problemas e todo mundo fica bem. Os escroques sao so' a gengiva que segura o dente, controlando as comunicacoes a prova de escuta eletronica dos bandidos.

E' uma ficcao, mas que ilustra bem as possibilidades de um novo tipo de guerra onde as vitimas nao irao morrer por meio de explosivos. Serao paralisadas p intermedio de virus de computador, distribuidos talvez dentro de software comercial e/ou sharware. Os computadores encarregados das financas serao inutilizados, gerando panico, confusao e desconfianca. As comunicacoes tambem seriam prejudicadas ou mesmo igualmente paralisadas. Uma vitoria ou derrota obtida atraves de uma devastacao silenciosa, nao violenta, mas humilhante e completa.

O DIREITO DO CIBERESPACO

Edgard Pitta de Almeida (1) - publicado c. a permissao do autor (q. na verdade ia me mandar uma versao mais enxuta, mas acabei perdendo contato e p mandar isso logo p publico, vai a versao original)

Sumario
A questao que se coloca e se o aprimoramento das tecnologias de transmissao eletronica de dados e a ligacao dos computadores pessoais em redes mundiais do tipo da Internet e outras, fara necessario o estabelecimento de novas regras juridicas ou se as normas existentes podem ser adaptadas para regular as novas situacoes.

A explosao das redes

Se 1995 foi o ano do grande boom da Internet(2) no mundo, em 1996 assistiremos a sua consolidacao como "o" meio de comunicacao. A grande rede, que surgiu com propositos militares no fim da decada de 60 e que durante muito tempo somente foi usado pela comunidade academica, popularizou-se de forma tal, que foi alcada a categoria de personagem de filmes, livros e ate de novela de televisao.

No Brasil, apesar de todas as dificuldades de estrutura, principalmente

pela carencia de linhas telefonicas e a baixa velocidade de transmissao dos dados, a situacao nao e diferente. Ja sao cerca de 180.000 usuarios cadastrados, atraves de mais de 300 provedores de acesso puAblicos e privados em todo o pais. Embora a maioria dos provedores esteja localizada no eixo Rio-Sao Paulo, praticamente todas as capitais do pais ja dispoem de provedores e ha casos de cidades do interior, como Blumenau-SC, que tem 5 provedores de acesso.

Da mesma forma, a quantidade de BBS(3) (Bulletin Board System) existentes e impressionante: sao cerca de 150, em todo o pais, e esse nuAmero nao para de crescer. Somente em Sao Paulo, onde se concentra a maior parte deles, ha BBS especificos para praticamente todos os gostos e necessidades, desde os genericos como o Mandic e o Comet, ate os dedicados a astrologia eesoterismo (Alto Astral), cristaos ciberneticos (Christian), previsao do tempo (Climatempo), informacoes financeiras e empresarias (Codep, DialData), cultura gay (Mix Brasil e GLS Connect), suporte on-line de empresas de computacao (Microsoft, IBM, Viruscan), informacoes juridicas (Lex= BBS), entre dezenas de outros, quase todos com recurso de CHAT, que permite bate-papo on-line entre usuarios.

Mas o que se faz, finalmente, na Internet ou num BBS? Ou melhor, com que objetivo se conectam computadores numa rede?

Basicamente, uma rede, qualquer que seja a tecnologia utilizada, tem por objetivo compartilhar recursos e facilitar a comunicacao entre os usuarios. Assim, e possivel trocar correspondencia eletronica (como se fosse atraves do correio), "conversar" com outros usuarios ao redor do mundo, em tempo real (em viva-voz, como pelo telefone, ou "por escrito"), assistir, ou acessar, informacoes graficas (como na televisao), gravar e utilizar softwares dos mais diferentes tipos, fazer reservas aereas, em hoteis e restaurantes, ler as uAltimas noticias nos principais jornais do mundo, alem de se adquirir produtos e servicos dos tipos mais variados, so para citar as possibilidades mais obvias.

Pode-se tambem difamar alguem ou ameaca-lo de morte, como no recente episodio em que foi divulgado um plano minucioso para assassinar a atriz americana Jodie Foster, atraves de um grupo de discussao (newsgroup); divulgar material pornografico ou atentatorio a moral ou a seguranca; invadir uma rede de computadores particular e apropriar-se indevidamente de dados sigilosos; violar copyrights, entre outros crimes e contravencoes.

Em resumo, numa rede deste tipo transmitem-se dados, em forma de texto ou digitalizada(4) , em ambas as direcoes, i. e., do computador remoto (host) para o usuario local (client) e vice-versa. Ora, dados tambem sao transmitidos atraves do correio, do telegrafo, do telex, do telefone, do radio e da televisao e nem por isso se cogitou da criacao de um ramo autonomo do direito especificamente dedicado a regular as relacoes, comerciais ou nao, decorrentes da utilizacao dessas midias(5).

Seguindo nesse raciocinio, as novas situacoes decorrentes da utilizacao da rede, poderiam ser plenamente reguladas pelas regras antigas, mediante uma nova interpretacao, eventualmente mais extensiva e adequada as= inovacoes tecnologicas.

Por exemplo, a norma constitutucional que preve a imunidade tributaria para o livro e o papel destinado a sua impressao poderia ser interpretada extensivamente de forma a abranger os livros publicados em meio eletronico, tal como o CD-ROM. Parece obvio? Nao o e para o fisco fluminense que entende que "o livro eletronico tem caracteristicas de software e quando vendido ja pronto e em serie deve ser considerado uma mercadoria, tendo como base de calculo o valor total, composto pelo suporte fisico e seu

conteudo.

Ainda que contenha as mesmas informacoes publicadas num livro, o programa de computador e completamente distinto" (?!) (grifou-se).

Neste caso especifico, a despeito do brilhante posicionamento do fisco estadual, alguns contribuintes ja vem obtendo exito em suas acoes no Judiciario sob a alegacao obvia de que as imunidades devem ser interpretadas extensivamente. Mas e se se tratasse de uma isencao, que, como sabemos, e interpretada restritivamente, a questao seria de tao clara resolucao?

Uma outra questao bem interessante diz respeito a tributacao da prestacao de servicos pelo ISSQN. Toda a sistematica de cobranca deste imposto esta baseada no conceito de local do estabelecimento prestador, ou do domicilio do prestador dos servicos, na inexistencia daquele. A questao se complica no caso dos prestadores de servicos on line, que nao tem estabelecimento fisico, nem sequer nuAmeros de telefone, mas somente um endereco virtual na rede. Esse site pode perfeitamente ser considerado o estabelecimento do prestador: ali ele e encontrado para todos os fins e atraves dele os servicos sao contratados. Quando possivel, as partes sequer se encontrarao ou se falarao, sendo o servico enviado por via eletronica, diretamente para o e-mail do beneficiario.

E' bem verdade que o fisco pode chegar ao domicilio do prestador, mas este pode alegar que tem um estabelecimento "virtual", o qual esta alocado no provedor "x", que por sua vez esta estabelecido fisicamente em outro municipio, ou mesmo outro pais, fora da jurisdicao daquele municipio.
Por outro lado, ab absurdo, o municipio em que estiver localizado o computador hospedeiro desses sites comerciais podera entender que, "fisicamente", estes "estabelecimentos virtuais" estao situados naquele local, e podera pretender cobrar imposto sobre as transacoes realizadas atraves daquele equipamento. Absurdo e fantasioso? Todos nos conhecemos a voracidade do fisco...

A questao da protecao aos direitos da personalidade e da honra tambem e bastante controversa. Ao acessar algum desses servicos on-line, o usuario pode cadastrar-se com seu nome real ou outro a sua escolha (pseudo ou nickname), atraves do qual sera conhecido pelos outros usuarios do servico. Caso opte por um nome ficticio, os outros usuarios jamais saberao seu nome verdadeiro.

A questao e se este pseudonimo e passivel de protecao legal.

Ou seja, alguem pode buscar protecao judicial por sentir-se injuriado ou difamado no seu user id, atraves do qual e conhecido naquela comunidade virtual? A opiniao de alguns colegas com quem discuti a questao e no sentido de nao aceitar a protecao legal ao pseudonimo, ja que na "vida real" a pessoa e conhecida pelo seu "nome real", e a protecao legal somente alcancaria este.

Pergunte, entretanto, a qualquer netizen(6) o que e mais importante para ele: seu "nome real" ou seu "nome virtual" ...

Pelos exemplos citados, entendo que o ponto-chave da discussao nao e saber se uma nova interpretacao das leis existentes seria suficiente para regular as novas situacoes, mas se estas regras sao adequadas a nova realidade.

Uma nova "realidade"?
Ora, o direito nao existe independentemente da realidade a que se propoe regular e o fato e que estamos vivendo numa nova realidade, a virtual. A dificuldade ja comeca em tentar conciliar dois termos, "realidade" e "virtual", aparentemente auto-exclusivos, etimologica e conceitualmente:

"realidade" implica uma ideia de coisa palpavel, enquanto "virtual" e algo que existe apenas idealmente.

O fato e que a realidade virtual, em oposicao a "realidade real" veio para ficar, ou como preve o prof. Nicholas Negroponte, um dos gurus dessa nova era (sao tantas), "Os atomos serao substituidos pelos bits" (7).

Segundo ele, as informacoes que as pessoas hoje recebem em forma de material palpavel (atomos), passarao a chegar sob forma de bits de informatica. Ressalte-se que essa tendencia afeta inclusive as relacoes interpessoais. A utilizacao de teleconferencias em substituicao a viagens de negocios ja e pratica corriqueira, mesmo no Brasil.

Nesse contexto, temos que analisar as consequCencias no mundo do direito da substituicao do "fisico" pelo "virtual", notadamente no que se refere aos aspectos espacial e temporal de criacao da lei e sua aplicacao.

Ciberespaco e Cibertempo

O direito e limitado pelo tempo e pelo espaco, aspectos verdadeiramente indissociaveis a sua natureza. O aspecto espacial, considerado na criacao e aplicacao do direito talvez seja o mais atingido pelas alteracoes tecnologicas. Todos nos aprendemos na Faculdade que a lei, como expressao da vontade soberana do povo politicamente organizado no Estado, obriga em um territorio fisico determinado, assim entendido como a parte do espaco sobre a qual o Estado exerce a sua soberania, o que compreende nao so o solo e sub-solo, mas o espaco aereo e o mar territorial, alem das aeronaves e belonaves, independente de onde estiverem, e os edificios diplomaticos (8).

Os conceitos de territorio fisico e de soberania, entretanto, deixam de fazer sentido no mundo virtual. Quando se acessa uma determinada informacao disponivel na rede, o usuario nao esta interessado em saber onde aquele computador esta localizado, nem por quantos paises aquela informacao vai trafegar ate chegar ao seu computador. Ou seja, as novas tecnologias de transmissao de dados atraves das redes de comunicacao derrubam por terra as fronteiras fisicas entre os Estados.

Com a queda dessas barreiras no plano virtual, os conflitos entre as normas juridicas existentes nos diversos paises diversos tendem a se= manifestar, o mesmo ocorrendo nos estados federativos, com o embaralhamento das esferas de competencia da uniao, dos estados e do municipios, como no exemplo do ISS citado.

Em sintese, ha que se dar um novo tratamento as varias questoes e conceitos que o direito descreve e define em termos espaciais, como e. g., a privacidade, que envolve uma ideia abstrata, mas tambem uma ideia espacial, e mesmo o conceito de jurisdicao, que e estritamente espacial.

Entendo, assim, que um novo conceito de espaco se faz necessario para fins de tutela juridica na sociedade virtual, o ciberespaco (9).

O outro aspecto a ser relevado e a questao temporal. O direito emprega o tempo, invoca o tempo e tem expectativas a respeito do tempo (10). A lei obriga em um determinado tempo; o "fluxo" do tempo e contado, suspenso e interrompido; direitos sao extintos e prescritos em funcao do fluir do tempo, ou seja, e impossivel isolar o direito da ideia de tempo. e' bem verdade que o direito nao pode fazer o tempo parar, nem voltar atras, mas pode "parar o tempo" na contagem de prazos ou retroagir para regular de forma diferente situacoes ja passadas.

Ou seja, o tempo nao e apenas uma grandeza fisica, fixa e imutavel. Mas e tambem um artefato cultural, e tambem a percepcao que temos do seu papel e do seu valor. A percepcao que temos do tempo esta, no mais das vezes, intimamente relacionada a velocidade com que os fatos chegam ate nos. Com a rapidez das novas tecnologias de transmissao de dados, as "distancias" temporais sao encurtadas, de modo que algo que so nos chegaria no "futuro", nos e trazido no presente, no momento exato em que esta acontecendo. Todos nos pudemos assistir pela TV, confortavelmente instalados na poltrona denossas salas, uma guerra acontecer em tempo real, a Guerra do Golfo Persico. O impacto seria o mesmo se tivessemos que esperar pela edicao semanal de O Cruzeiro para ler as uAltimas noticias?

A percepcao do tempo, assim como do espaco, definitivamente passou a ter outro valor. O que implica dizer que estamos diante de uma nova ideia de tempo como artefato cultural: o cibertempo. Ou como afirma o prof. Kastch, o cibertempo esta para o tempo, como o ciberespaco esta para o espaco(11). Na verdade, nao se trata de dizer que o cibertempo implica simplesmente numa aceleracao dos processos relativos a transmissao de dados ou numa nova maneira de "medir" o tempo. Implica principalmente numa nova percepcao do papel e do valor das ideias de passado, presente e futuro (12).

O Direito do Ciberespaco

Em funcao desses questionamentos, facilmente podemos vislumbrar que as regras aplicaveis as relacoes juridicas no espaco fisico e temporal, da forma como foi construida toda a teoria do direito ate entao, nao podem ser as mesmas aplicaveis no espaco virtual, ou ciberespaco, sem considerar as profundas diferencas existentes entre a realidade "real" e a "virtual". Entendo, assim, que um novo ramo do direito, ou pelo menos um novo conjunto de regras baseado no conceito de cibertempo e ciberespaco, ira surgir.

Direito da informatica (denominacao utilizada por alguns juristas e advogados brasileiros), direito informatico (como usam os argentinos)(13), direito das telecomunicacoes, direito "on line", tem sido algumas das denominacoes dadas a esse novo conjunto de regras. A denominacao que mais me agrada e direito do ciberespaco (cyberspace law ou cyberlaw, dos americanos), assim entendido como o conjunto das normas que regem as relacoes juridicas que surgem em decorrencia da entrada das pessoas no espaco das redes de computador - o ciberespaco. Com a utilizacao desse termo, pretendo que fique claro que as novas regras sao aplicadas na medida,e somente na medida, em que as pessoas se logam (14) a uma rede e estao "on line"(15).

Exponho a seguir algumas materias que tem sido objeto de discussao e de conflitos no ciberespaco, as quais entendendo necessitam de regulamentacao mais apropriada (16):

* Jurisdicao: O conceito de jurisdicao e, sem duAvida, o mais afetado pela utilizacao macica das redes. Tratas-se, pois, de determinar que leis serao aplicaveis no ciberespaco, num determinado momento do tempo. Principios basicos de direito internacional e federalismo podem ser uAteis na tarefa.

* Protecao Legal e Sancoes: O direito criminal do ciberespaco. Algumas praticas criminosas as vezes apenas violam, atraves de um novo meio (o computador, ou o computador combinado com o sistema telefonico), direitos ja tutelados pela ordem juridica, caso em que se trata apenas de dar uma nova interpretacao as regras existentes. Entretanto, nem sempre

essa coneccao e possivel, ou mesmo desejavel, merecendo nova regulamentacao.

A nova fauna de viciados em computador, denominada genericamente de ciberpunks, engloba desde os inofensivos hackers (17), ravers (18) e cipherpunks(19) , os nem sempre inofensivos phreaks(20) , ate os mais perigosos crackers (21), que invadem sistemas alheios para ganho ilicito ou por simples prazer de exercitar suas habilidades, criam e disseminam virus de computador de potencial destrutivo inimaginavel, entre outras atividades.

* Propriedade Intelectual: Os direitos de propriedade intelectual, protegidos atraves de patentes, marcas registradas de comercio e induAstria, direitos de reproducao, institutos ja conhecidos antigos nossos, merecem um novo tratamento. Por outro lado, novas criacoes merecem regulamentacao, como os bancos de dados informatizados, com dados puAblicos, que nao se encaixam no conceito atualmente passivel de protecao legal.

Nao se pode deixar de considerar tambem a revisao dos prazos de protecao legal desses direitos e mesmo se essa protecao faz sentido no ciberespaco.

* Transacoes Comerciais: Talvez o lado mais badalado dos servicos on line. Hoje e possivel adquirir os mais diferentes produtos e servicos diretamente da rede e o preco ser debitado no cartao de credito automaticamente. As velhas regras do direito comercial e as inovacoes na protecao ao consumidor, tem que ser revistas no novo paradigma.

* Privacidade: A questao do direito a privacidade trata de estabelecer medidas de protecao a liberdade individual numa nova realidade repleta de facilidades para monitorar as atividades dos individuos. Monitorar toda a correspondencia eletronica de alguem, de forma absolutamente segura e secreta, por exemplo, e imensamente mais facil que monitorar a correspondencia escrita e comunicacao telefonica. Manter bancos de dados extremamente precisos, sobre uma parcela bastante grande da populacao,tambem e algo facilmente realizavel.

Envolve, tambem, a questao da distribuicao dos programas de criptografia e dos esforcos dos governos (basicamente o governo americano) em estabelecer padroes criptograficos. O criador do programa de criptografia Pretty Good Privacy - PGP, o mais disseminado e de uso mais facil, Philip Zimmerman, chegou a ser processado pelo governo americano sob a acusacao de exportacao de armamentos, ja que nos EUA os programas de criptografia recebem o mesmo tratamento legal das armas (nao podemos esquecer quer os primeiros computadores foram desenvolvidos em segredo, no final da Segunda Guerra Mundial, com o objetivo principal de quebrar codigos do inimigos). Tanto que nao se consegue, partindo de um endereco eletronico de fora do EUA, baixar pela Internet nenhum programa de criptografia que esteja armazenado em um computador americano. Nem por isso esses programas deixaram de circular livremente no resto do mundo, podendo ser facilmente baixados em qualquer BBS de Sao Paulo.

Conclusao

Diante dos fatos e razoes expostos, entendo que um novo conjunto de normas comeca a surgir: normas baseadas nos conceitos de cibertempo e ciberespaco, para aplicacao especifica na sociedade virtual que se forma nas grandes redes de comunicacao, mundiais ou locais. Fechar os olhos para essa nova realidade, pode significar perder mais uma vez o bonde da historia, como aconteceu com os anos em que o Brasil fechou-se ao que acontecia no resto

do mundo em materia de informatica em decorrencia da reserva de mercado.

NOTAS

1. Edgard Pitta de Almeida, consultor tributario no escritorio Gaia, Silva, Rolim & Associados. Graduado em direito pela Universidade Catolica do Salvador - BA e atualmente cursando pos-graduacao em Administracao (CEAG) na Fundacao GetuAlio Vargas - Sao Paulo-SP. e-mail Internet: ealmeid@amcham.com.br
2. A Internet e uma grande rede de computadores, que conecta, segunda estimativas, mais de 40 milhoes de computadores, de todos os portes, ao redor do mundo. e' resultado da combinacao de duas tecnologias: computacao e telecomunicacoes.
3. Os Bulletin Board Systems (BBS) surgiram com um meio de disseminar mensagens entre os diversos usuarios de uma rede. Atualmente, funcionam atraves de um computador central, ao qual os usuarios se conectam por via telefonica, podendo trocar mensagens com os outros usuarios, copiar arquivos de textos ou de programas, entre outras coisas.
4. A informacao digitalizada que foi desmaterializada em uma serie de pulsos binarios on/off (ligado/desligado) ou representados por 0 e 1.
5. O uso do termo "midia", no singular, como sinonimo de meio de comunicacao, apesar de incorreto etimologicamente, ja se tornou corrente em portugues.
6. Neologismo resultado da fusao de net (rede) com citizen (cidadao)
7. NEGROPONTE, Nicholas - A Vida Digital, 1995
8. RAO, Vicente - O Direito e a vida dos direitos, cap. 13
9. Embora o conceito tenha surgido antes, o termo cyberspace foi primeiramente utilizado pelo escritor americano Willian Gibson em seu romance "Burning Chrome". Ciberespaco pode ser definido como o "local" metaforico em que alguem se encontra quando "esta" acessando o mundo das redes de computador. e' utilizado tambem para denominar qualquer ambiente gerado por realidade virtual, mesmo que o objetivo nao seja acessar alguma rede. Informacoes retiradas do FAQ (Questoes FrequCentemente Feitas) sobre alt.cyberpunk, montado por Erich Schneider (erich@bush.cs.tamu.edu). Versao ASCII atualizada disponivel por FTP anonimo em e versao HTML no URL

10. KATSCH, M. Ethan - Cybertime, Cyberspace and Cyberlaw, 1995 J. Online L. art. 1 - Disponivel no URL:

11. KATSCH. id., ib.
12. KATSCH, id., ib.
13. Derecho Informatico Buenos Aires: Depalma, 1994, p.56 - apud Edvaldo Brito, Software: ICMS, ISS ou Imunidade Tributaria? in Revista Dialetica de Direito Tributario n 5, 1996
14. Traducao da expressao inglesa "log in", que significa obter acesso a um sistema, normalmente atraves de uma senha, traduzido para o portugues como "logar". Perdoem-me pelo uso excessivo de expressoes inglesas, mas quem importa tecnologia, termina por importar tambem o vocabulario tecnico.
15. Diz-se que alguem esta "on line", no momento em esta acessando alguma rede de computador.
16. Utilizo, com adaptacoes, o conteuAdo proposto pelo UCLA Online Institute for Cyberspace and Policy, que reuAne em seu board os principais estudiosos americanos do cyberlaw. O site do Instituto e no URL .
17. Hackers sao os magos dos computadores; pessoas com um profundo entendimento de como os computadores funcionam e que podem fazer coisas com eles que parecem "magicas". FAQ on alt.cyberpunk, ibidem.
18. Grupo que ouve muAsica sintetizada e sampleada e gosta de arte

psicodelica gerada por computador. A uAnica contravencao que praticam e usar drogas alucinogenas, tipo o Ecstasy, para embalar as festas realizadas em galpoes abandonados (raves), que duram toda a noite. FAQ on alt.cyberpunk, ibidem.
19. Fanaticos por encriptacao de mensagens. Acreditam que o uso massivo de sistemas de encriptacao de dificil (leia-se, virtualmente impossivel) quebra criara "regioes de privacidade" que "O Sistema" nao podera invadir. FAQ on alt.cyberpunk, ibidem.
20. Grupo que usa o sistema telefonico para invadir os computadores das proprias companhias telefonicas para trocar contas telefonicas e praticar atos nem sempre licitos atraves do sistema telefonico. FAQ on alt.cyberpunk, ibidem.
21. FAQ on alt.cyberpunk, ibidem.

Edgard Pitta de Almeida
Sao Paulo-SP BRASIL
ealmeid@amcham.com.br
=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=

AJUDE KEVIN!

Kevin David Mitnick, nascido em Van Nuys, California em 06.08.63. Preso em 15.02.94 sob alegacao de violacao de condicional, acesso nao autorizado a sistemas de comunicacao, entre outras acusacoes. Encontra-se detido atualmente no Metropolitan Detention Center, de Los Angeles, California.

Meu nome e Fernanda Serpa, sou ativista de direitos humanos e membro da Anistia Internacional. Juntamente com dois amigos, Gustavo Weide, tecnico em computacao e Ana Elisa Prates, ativista de direitos humanos, estamos iniciando uma campanha a nivel mundial para assegurar ao "hacker" Kevin David Mitnick, um julgamento justo e condicoes carcerarias saudaveis de acordo com a Declaracao Universal dos Direitos Humanos, em especial nos seus artigos V, VI, VII, VIII, X, XI-1 e 2 que vem sendo sistematicamente violados no caso em questao. De acordo com a imprensa americana e internacional, Kevin David Mitnick foi preso sob condicoes ilegais contrariando a Declaracao Universal dos Direitos Humanos e a propria Constituicao Americana. A grande "cacada eletronica" desencadeada contra Mitnick expos inclusive a tenue linha que separa os direitos constitucionais da privacidade com o cumprimento das leis que, parece, foram violadas em nome da suposta "ameaca" chamada Kevin Mitnick.

Preocupacao por maus tratos

Kevin Mitnick ja teve seus direitos violados quando da sua prisao anterior em dezembro de 1988. Foi negada sua fianca apesar da legislacao americana afirmar que a Lei Federal so "considera perigoso para a sociedade o reu que foi acusado de crime violento, crime

capital ou crime relacionado com drogas envolvendo uma sentenca de mais de dez anos".

Trecho do livro de Jonathan Littman - "O Jogo do Fugitivo - Em linha direta com Kevin Mitnick":

"Ele cumpriu oito meses na solitaria no Centro Metropolitano de Detencao de Los Angeles e quatro meses em Lompoc, perto da costa, onde conheceu Ivan Boesky. Depois, apos seis meses numa residencia judia de transicao para o retorno a sociedade, Kevin Mitnick tentou reingressar na forca de trabalho. Conseguiu um lugar de programador em Las Vegas, mas seu empregador tinha tanto medo da sua reputacao que ele nao podia ficar sozinho na sala dos computadores. Pela lei, Mitnick teve de contar que era um ex-condenado.

Finalmente, depois que perdeu o emprego de programador em Las Vegas, em junho de 1991, Mitnick convenceu-se de que seus esforcos eram em vao. Ele candidatou-se a emprego em todos os cassinos informatizados: Caesar's, Mirage, Sands. Todos pareciam interessados, ate que seu agente da condicional telefonava ou escrevia.

O governo federal decidira que Kevin Mitnick era um perigo para a sociedade, e, como um estuprador condenado ou um molestador de criancas, ele era monitorado. Seu agente da condicional entrava persistentemente em contato com os possiveis empregadores: 'Ele tem acesso a dinheiro em especie? Quero que o senhor compreenda o perigo...' ".

Fala Kevin Mitnick no mesmo livro:

" - Cumpri oito meses no MDC (Metropolitan Detention Center - Los Angeles). A solitaria era um inferno. Diziam que eu era demasiado perigoso para chegar perto de um telefone. Deixavam que eu saisse uma hora por dia. Algemam voce quando o levam para o banho. e' como no cinema. Tratam voce como um animal. Um so dia ja e o inferno. Imagine oito meses. Ferram com as pessoas."

Como esta Kevin agora? Nao sabemos... A julgar pelo tratamento degradante a que foi submetido anteriormente, teme-se por maus tratos.

Um hacker ao velho estilo

Durante a perseguicao iniciada em novembro de 1992 (apos a expedicao de mandado de prisao por violacao de condicional), e que culminou em sua prisao em 15 de fevereiro de 1994, Kevin Mitnick persistiu trabalhando, fazendo bicos para sobreviver. A motivacao de Kevin para a "pirataria eletronica compulsiva" nunca foi o dinheiro. Nunca usou de forma criminosa seus conhecimentos. Kevin Mitnick nunca incitou nem cometeu atos de violencia. Kevin David Mitnick e um hacker. Na definicao de Jonathan Littman "um hacker ao velho estilo - Alguem que criativamente persegue conhecimento e informacao".

Direitos Humanos em Movimento

Que o Governo e a sociedade americana deem a Kevin Mitnick uma real chance de reabilitacao na sociedade e apenas uma esperanca. Mas EXIGIR que o Estado lhe de um julgamento justo e condicoes carcerarias saudaveis e uma realidade: VOCe pode fazer isto escrevendo apelos para a Ministra da Justica Americana, Ms. Janet Reno. Ja comecamos nossa campanha "Ajude Kevin" enviando a seguinte carta:

MS. JANET RENO
United States Secretary of Justice
Department of Justice
10th E. Constitution Ave, N.W., Room 4400
Washington, D.C. 20530

Prezada Senhora:

De acordo com a imprensa de seu proprio pais e a imprensa internacional, o Sr. Kevin David Mitnick foi preso sob condicoes ilegais contrariando a Declaracao Universal dos Direitos Humanos e a propria Constituicao Americana. O mesmo encontra-se recluso no Metropolitan Detention Center, em Los angeles, California.

Escrevo para solicitar a V.Exa. que assegure um julgamento justo e condicoes carcerarias saudaveis para o Sr. Kevin David Mitnick. Minha preocupacao e baseada em principios humanisticos e fundamentais do Direito Internacional.

Atenciosamente,

_____
Assinatura

Nota: Voce pode escreve-la em portugues ou preferencialmente em ingles, acessando o seguinte endereco:
http://www.angelfire.com/pg0/mitnick/english.html

O importante e fazer a carta e envia-la o mais breve possivel pelo Correio. Peca a seus amigos, parentes, conhecidos, amigos da Internet para fazerem o mesmo. Sua carta se juntara a muitas outras e sem dzvida esta pressao ratificara o desejo de todos de fazer com que a Declaracao Universal dos Direitos Humanos seja uma realidade em movimento. Para Kevin Mitnick. Para todos. Sem distincao.

Abracos,
Fernanda Serpa e equipe.

Se voce quiser entrar em contato conosco o E-mail e :
g_weide@portoweb.com.br

PGP PARA NOVATOS

Se ha' uma coisa que me da' uma certa frustracao, e' que os fucadores brasileiros nao manjam de criptografia. As vezes recebo perguntas muito, mas muito inteligentes. Mas a pessoa me manda tudo sem ser encriptado. Como e' que vou responder uma coisa que meu sysop sabe que foi perguntado a mim? E' nojento. So' eu e a pessoa com quem estou conversando podem saber qual o objetivo da conversa. Como conseguir isso? Via um o PGP, ou Pretty Good Privacy, um programinha americano capaz da magica de permitir que duas pessoas troquem correspondencia eletronica sem precisar se preocupar em ter o sysop lendo tudo. Como conseguir o dito?

ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP/
ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/
ftp://ftp.csua.berkeley.edu/pub/cypherpunks/pgp/

Observacao:

Existe a versao norueguesa do PGP, que tem a grande vantagem de nao entrar em choque com a questao de patente da americana.

WWW:
http://www.ifi.uio.no/pgp/

FTP:
ftp.ifi.uio.no/pub/pgp/

E-mail:
Mande mensagem para pgp@hypnotech.com e coloque seu pedido no campo de Subject.

Subject	Voce recebe
GET pgp263i.zip	MS-DOS executavel (uuencodado)
GET pgp263ix.zip	32-bit MS-DOS executavel (uuencodado)
GET pgp263i-os2.zip	OS/2 executavel (uuencodado)
GET pgp263i-win32.zip	Windows 95/NT text-mode executavel (uuencodado)

(Pode parecer brincadeira, mas e' serio. Nao faca download
do PGP a partir de sites americanos).

Primeiros passos:

Para dar inicio a coisa, e' necessario descompactar o programa com a seguinte linha de comando:

pkunzip -d pgp263i.zip

A primeira fase, depois do programa descompactado, e' a criacao ou geracao da chave secreta de descriptografacao. Quale' esse lance? Sao duas senhas que sao usadas num sistema de comunicacao via pgp. Uma e' a senha publica, melhor conhecida como chave publica, que pode ser distribuida para todo mundo. Outra senha (ou chave) e' a chave privada. Pois bem, todas as duas sao geradas uma unica vez (na verdade, a pessoa tenta umas cinco ou seis vezes, quando acha que aprendeu, repete o processo mais uma vez e ai entao esquece esse negocio de "gerar chave publica e privada").
Para poder gerar suas duas chaves, digite a linha de comando:

pgp -kg

Outra coisa e' a variavel tz. E' preciso "setar" a variavel. Pode colocar:

set tz=0

Chamando de novo (pgp -kg), basicamente e' preciso responder as perguntas do programa, tais como nome do usuario, informacoes, correio eletronico, etc. Ai' o programa ira' pedir uma frase-senha. Essa frase senha pode ate' ter 128 letras.

O programa vai te perguntar qual o tipo de criptografacao voce quer. Peca a mais foda, de 1024.

Duvidas: copie a versao em portugues do manual no http://www.geocities.com/SiliconValley/5620/misc.html e leia.

O resultado serao dois arquivos:

secring.pgp e o pubring.pgp

O primeiro, e' pra guardar a sete chaves. O segundo e' o q. voce pode distribuir (mais ou menos, tem um criterio p. isso) publicamente. E' bom fazer back-up.

Para criar um arquivo de "pgp-public-key-ring" pronto p. ser enviado p. email:

pgp -kxa

O programa vai perguntar o arquivo de saida que e' chamado de "armoured". Pode ser enviado sem medo pela internet.

Como e' que se envia uma mensagem criptografada por pgp, via email?

Vamos supor:

Voce quer escrever uma mensagem p. o Derneval, do Barata Eletrica. Depois de descobrir que a chave pgp esta' em alguns dos primeiros numeros do BE, edita ou apaga tudo, menos o seguinte texto:

```
----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6

mQCNAi7UlucAAAEEAM/eXiKMcvB2vmomVMBZYewgc66WRZcE9MNaXdLKIWSJo3vR
FSeLtBvSfr0kvzZzWJW38uLWT3OIM/kJ5CX6C35kksdNjipUXZ2hbXazvReGE/Of
t5o9SRe2l4QbQoAmYXm/B4TNs99fUmtWZCc3HWlXmUbDtMTJzyqI+aKIaaVdAAUR
tD1EZXJuZXZhbCBSaWJlaXJvIFJvZHJpZ3VlcyBkYSBDdW5oYSA8cm9kcmlnZGVA
Y2F0LmNjZS51c3AuYnI+
=56Ma
-----END PGP PUBLIC KEY BLOCK-----
```

salva como derneval.asc

digita:

pgp derneval.asc

O programa vai perguntar se voce quer adicionar essa chave ao seu pubring.pgp . Se esta' inseguro, responda sim (voce salvou o backup dos arquivos pubring.pgp e o secring.pgp, nao salvou?) pode ser q. ele faca outra pergunta sobre certificacao de chave. Se voce nao souber o que e' isso, responda nao. Se quiser saber o que e', leia o manual.

Ai' digita:

pgp -ea derneval

O programa vai comecar a criptografar a mensagem de uma forma q. so o usuario final (eu, no caso) possa ler. E' legal que o remetente possa ler e o pgp permite criptografar p. mais de uma pessoa.

pgp -ea derneval

Como e' que descriptografo o arquivo q. recebi?

pgp arquivo.txt

O programa vai pedir a frase senha.

Detalhe: isso vai acontecer se o pgp encontrar o arquivo secring.pgp no mesmo subdiretorio.

Falar sobre o PGP e' objeto para um livro. Sempre resisti a ideia de explicar em poucas palavras porque achei que fucador de micro nao podia ser preguicoso quanto a seguranca de sua comunicacao. Mas o tempo me ensinou que nao e' assim. Por isso recomendo a leitura do manual do usuario.

ALGUMAS FONTES DE INFORMACAO E SITES

FAQs:

    PGP Frequently Asked Questions
      http://www.prairienet.org/~jalicqui/pgpfaq.txt
      ftp://ftp.prairienet.org/pub/providers/pgp/pgpfaq.txt
    Where to Get the Latest PGP Program FAQ
      ftp://ftp.uu.net/usenet/news.answers/pgp-faq/where-is-PGP.Z

BREVE REFERENCIA DO PGP

Aqui esta' um breve resumo dos comandos do PGP.

Para criptografar um arquivo de texto plano com a chave publica do destinatario:

        pgp -e arquivo_texto userID_do_destinatario

Para assinar um arquivo de texto plano com sua chave secreta:

        pgp -s arquivo_texto [-u seu_userID]

Para assinar um arquivo de texto plano ASCII com sua chave secreta, produzindo uma mensagem de texto plano assinada (nao-criptografada) adequada para ser enviada via correio eletronico:

        pgp -sta arquivo_texto [-u seu_userID]

Para assinar um arquivo de texto plano com sua chave secreta e depois criptografa-lo com a chave publica do destinatario:

        pgp -es arquivo_texto userId_do_destinatario [-u seu_userID]

Para criptografar um arquivo de texto plano somente com a criptografia convencional, digite:

```
        pgp -c  arquivo_texto
```

Para descriptografar um arquivo criptografado ou para verificar a integridade da assinatura de um arquivo assinado:

```
        pgp  arquivo_de_texto_codigo  [-o arquivo_de_texto_plano]
```

Para criptografar uma mensagem para varios destinatarios multiplos:

```
        pgp -e  arquivo_texto  userID1  userID2  userID3
```

--- Comandos de administracao de chaves:

Para gerar seu proprio par unico de chave publica/secreta:

```
        pgp -kg
```

Para acrescentar um conteudo do arquivo de chave secreta ou publica para seu anel de chave publica e secreta:

```
        pgp -ka  arquivo_de_chave  [anel_de_chave]
```

Para extrair (copiar) uma chave do seu anel de chave publica ou secreta:

```
        pgp -kx  userID arquivo_de_chave  [anel de chave]
```
ou:
```
        pgp -kxa  userID  arquivo_de_chave  [anel de chave]
```

Para ver os conteudos do seu anel de chave publica:

```
        pgp -kv[v]  [userID]  [anel_de_chave]
```

Para ver a "digital" de uma chave publica, a fim de verifica-la pelo telefone com seu dono:

```
        pgp -kvc  [userID]  [anel_de_chave]
```

Para ver os conteudos e verificar as assinaturas certificadas de seu anel de chave publica:

```
        pgp -kc  [userID]  [anel_de_chave]
```

Para editar o userID ou a frase senha para sua chave secreta:

```
        pgp -ke  userID  [anel_de_chave]
```

Para editar os parametros confiaveis para uma chave publica:

```
        pgp -ke  userID  [anel_de_chave]
```

Para remover uma chave ou apenas um userID de seu anel de chave publica:

```
        pgp -kr  userID  [anel_de_chave]
```

Para assinar e certificar a chave publica de alguem no seu anel de chave publica:

```
        pgp -ks  userID_do_destinatario  [-u seu_userID]  [anel_de_chave]
```

Para remover assinaturas selecionadas de um userID em um anel de chave:

```
        pgp -krs  userID  [anel_de_chave]
```

Para remover definitivamente sua propria chave, divulgando um certificado de comprometimento de chave:

```
        pgp -kd  seu_userID
```

Para invalidar ou reabilitar uma chave publica em seu proprio anel de chave publica:

```
         pgp -kd  userID
```

--- Comandos Esotericos:

Para descriptografar uma mensagem e deixar intacta sua assinatura:

```
        pgp -d  arquivo_de_texto_codigo
```

Para criar um certificado de assinatura que esta' separado do documento:

```
        pgp -sb  arquivo_texto  [-u seu_userID]
```

Para separar um certificado de assinatura de uma mensagem assinada:

```
        pgp -b  arquivo_de_texto_codigo
```

--- Opcoes de comandos que podem ser usados em combinacao com outras opcoes de comandos (algumas vezes ate' formam palavras interessantes!):

Para produzir um arquivo de texto codigo no formato ASCII Base-64, apenas acrescente a opcao -a quanto criptografar ou assinar uma mensagem ou extrair uma chave:

```
        pgp -sea  arquivo_texto  userId_do_destinatario
```

ou:

```
        pgp -kxa  userID  arquivo_de_chave  [anel_de_chave]
```

Para apagar o arquivo de texto plano depois de produzir o arquivo de texto codigo, apenas acrescente a opcao -w (wipe - destruir) quando criptografar ou assinar uma mensagem:

```
        pgp -sew  mensagem.txt  userID_do_destinatario
```

Para especificar que um arquivo de texto plano contem texto ASCII, nao binario, e que deveria ser convertido de acordo com os padroes locais de tela do destinatario, acrescente a opcao -t (texto) junto as outras opcoes:

```
        pgp -seat  mensagem.txt  userID_do_destinatario
```

Para ver a saida do texto plano criptografado na sua tela (como o comando "more" do estilo UNIX), sem escreve-lo em um arquivo, use a opcao -m (mais) quanto descriptografa:

```
        pgp -m  arquivo_de_texto_codigo
```

Para especificar que o texto plano descriptografado do destinatario sera' mostrado SOMENTE na tela dele e nao podera' ser salvo em disco, acrescente a opcao -m:

```
        pgp -steam  mensagem.txt  userID_do_destinatario
```

Para recuperar o nome original do arquivo de texto planto enquanto descriptografa, acrescente a opcao -p:

```
pgp -p  arquivo_de_texto_codigo
```

Para usar um filtro do estilo UNIX, lendo da entrada padrao e escrevendo para a saida padrao, acrescente a opcao -f:

```
pgp -feast userID_do_destinatario  arquivo_saida
```

Este resumo foi retirado do arquivo pgpdoc1.br, traduzido por:
ROBERTA PAIVA BORTOLOTTI
Revisao de Adriano Mauro Cansian
disponivel tambem no:
http://www.geocities.com/SiliconValley/5620/misc.html

HACKER MANIFESTO

Obs: Este texto foi escrito pelo Mentor, um dos hackers velha guarda (coisa de uns cinco, seis anos atras). Foi traduzido por Ricardo Jurczyk Pinheiro - jurczy@br.hommeshopping.com.br - Valeu a contribuicao.

Mais outro foi pego hoje, esta tudo nos papeis. "Adolescente preso em Escandalo do Crime de Computador", "Hacker preso apos trapaca em Banco"
de 3 angulos e cerebro de 1950, alguma vez olhou atras dos olhos de um hacker? Voce ja imaginou o que faz ele agir, quais forcas balancam ele, o que o tornou assim? Eu sou um Hacker, entre para o meu mundo...
Meu mundo e aquele que comeca com a escola... Eu sou mais esperto que os outros, esta besteira que nos ensinam, me aborrece... Cacete trapaceiro. Ele todos sao iguais. Eu estou no ginasio. Eu ouvi os professores explicarem pela quinquagesima vez como reduzir uma fracao. Eu entendo como. "Nao, Sra. Smith, eu nao mostrei meu trabalho. Eu fiz na minha cabeca..."
Cacete crianca. Provavelmente copiei. Ele sao todos iguais.
Eu fiz uma descoberta hoje. Eu encontrei um computador. Espere um pouco, Isto e bacana. Faz o que eu quero. Se cometer um erro e porque fudeu tudo. Nao porque ele nao gosta de mim... Ou se sente atraido por mim... Ou pense eu sou um CDF... Ou nao gosta de ensinar e nao gostaria de estar aqui. Cacete crianca. Tudo o que ele faz e jogar jogos. Eles sao todos iguais. E entao aquilo acontece... uma porta aberta ao mundo... surfando pela linha telefonica como heroina nas veias, um comando enviado, um refugo da incompetencia de procurar no dia-a-dia...
Uma BBS e achada. "e' isto... e' aqui que eu pertenco.
Eu conheco todo mundo aqui... Mesmo que eu nunca conheci eles, nunca conversei e ate nunca os vi... Eu conheco todos voces. Cacete crianca...
Enganando a linha telefonica de novo. Eles sao todos iguais... Aposte seu rabo que sao...
Nos fomos alimentados com comida de bebe na escola quando queriamos bifes... Os pedacos de carne que voce deixou escapar estavam pre-cozidos e sem gosto. Nos fomos dominados por sadicos, ou ignorados por pateticos. Os poucos que tiveram algo a nos ensinar quando eramos criancas, acharam-nos dispostos a tudo, mas estes sao como lagos d'agua no deserto.
Este e o nosso mundo agora... O mundo do eletron e da mudanca, a beleza d modem. Nos fazemos uso de um servico ja existente sem pagar por aquilo que seria bem caro se nao fosse usado por gulosos atras de lucros, e voces nos chamam de criminosos. Nos exploramos... e voces nos chamam de criminosos.
Nos procuramos por conhecimento... e voces nos chamam de criminosos. Nos existimos sem cor de pele, sem nacionalidade, sem religao... e voces nos

chamam de criminosos. Voces constroem bombas atomicas, voces comecam guerras, assassinam, trapaceam, e mentem para nos e tentam fazer que acreditamos que e para nosso proprio bem, sim, nos somos os criminosos.

Sim, eu sou um criminiso. Meu crime e o da curiosidade. Meu crime e o de julgar pessoas pelo o que elas dizem e pensam, nao como elas se parecem. Meu crime e de desafiar voces, algo que voces nunca me faram esquecer.
Eu sou um hacker e este e o meu manifesto. Voces tambem podem parar este individuo, mas nao podem parar todos nos... apesar de tudo, nos somos todos iguais.

+++The Mentor+++

STALKING THE WILY HACKER (CONTINUACAO)

INTRUDER'S INTENTIONS

Was the intruder actually spying? With thousands of military computer attached, MILNET might seem inviting to spies. After all, espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations. Further, it would seem to be insulated from risks of internationally embarrassing incidents. Certainly Western countries are at much greater risk than nations without well-developed computer infrastructures. Some may argue that it is ludicrous to hunt for classified information over MILNET because there is none. Regulations [21] prohibit classified computers from access via MILNET, and any data stored in MILNET systems must be unclassified. On the other hand, since these computers are not regularly checked, it is possible that some classified information resides on them. At least some data stored in these computers can be considered sensitive, especially when aggregated. Printouts of this intruder's activities seem to confirm this. Despite his efforts, he uncovered little information not already in the public domain, but that included abstracts of U.S. Army plans for nuclear, biological, and chemical warfare for central Europe. These abstracts were not classified, nor was their database. The intruder was extraordinarily careful to watch for anyone watching him. He always checked who was logged onto a system, and if a system manager was on, he quickly disconnected. He regularly scanned electronic mail for any hints that he had been discovered, looking for mention of his activities or stolen log-in names (often, by scanning for those words). He often changed his connection pathways and used a variety of different network user identifiers. Although arrogant from his successes, he was nevertheless careful to cover his tracks. Judging by the intruder's habits and knowledge, he is an experienced programmer who understands system administration. But he is by no means a "brilliant wizard," as might be popularly imagined. We did not see him plant viruses [18] or modify kernel code, nor did he find all existing security weaknesses in our systeM. He tried, however, to exploit problems in the UNIX/usr/spool/at [36], as well as a hole in the vi editor. These problems had been patched at our site long before, but they still exist in many other installations. Did the intruder cause damage? To his credit, he tried not to erase files and killed only a few processes. If we only count measurable losses and time as damage, he was fairly benign [41]. He only wasted systems staff time, computing resources, and network connection time, and racked up long-distance telephone tolls and international network charges. His liability under California law [6], for the costs of the computing and network time, and of tracking him, is over $100,000. But this is a narrow view of the damage. If we include intangible losses, the harm he caused was serious and deliberate. At the least, he was

trespassing, invading others' property and privacy; at worst, he was conducting espionage. He broke into dozens of computers, extracted confidential information, read personal mail, and modified system software. He risked injuring a medical patient and violated the trust of our network community. Money and time can be paid back. Once trust is broken, the open, cooperative character of our networks may be lost forever.

AFTERMATH: PICKING UP THE PIECES

Following successful traces, the FPI assured us teh intruder would not try to enter our system again. We began picking up the pieces and tightening our sytem. The only way to guarantee a clean system was to rebuild all systems from source code, change all passwords overnight, and recertify each user. With over a thousand users and dozens of computers, this was impractical, especially since we strive to supply our users with uninterrupted computing services. On the other hand, simply patching known holes or instituting a quick fix for stolen passwords [27] was not enough. We settled on instituting password expiration, deleting all expired accounts, eliminating shared accounts, continued monitoring of incoming traffic, setting alarms in certain places, and educating our users. Where necessary, system utilities were compared to fresh versions, and new utilities built. We changed network-access passwords and educated users about choosing nondictionary passwords. We did not institute random password assignment, having seen that users often store such passwords in command files or write them on their terminals. To further test the security of our system, we hired a summer student to probe it [2]. He discovered several elusive, site-specific security holes, as well as demonstrated more general problems, such as file scavenging. We would like to imagine that intruder problems have ended for us; sadly, they have not, forcing us to continue our watch.

REMAINING OPEN TO AN INTRUDER

Should we have remained open? A reasonable response to the detection of this attack might have been to disable the security hole and change all passwords. This would presumably have insulated us from the intruder and prevented him from using our computers to attack other internet sites. By remaining open, were we not a party to his attacks elsewhere, possibly incurring legal responsibility for damage? Had we closed up shop, we would not have risked embarrassment and could have resumed our usual activities. Closing up and keeping silent might have reduced adverse publicity, but would have done nothing to counter the serious problem of suspicious (and possibly malicious) offenders. Although many view the trace back and prosecution of intruders as a community service to network neighbors, this view is not universal [22]. Finally, had we closed up, how could we have been certain that we had eliminated the intruder? With hundreds of networked computers at LBL, it is nearly impossible to change all passwords on all computers. Perhaps he had planted subtle bugs or logic bombs in places we did not know about. Eliminating him from LBL would hardly have cut his access to MILNET. And, by disabling his access into our system, we would close our eyes to his activities; we could neither monitor him nor trace his connections in real-time. Tracing, catching, and prosecuting intruders are, unfortunately, necessary to discourage these vandals.

LEGAL RESPONSES

Several laws explicitly prohibit unauthorized entry into computers. Few states lack specific codes, but occasionally the crimes are to broadly

defined to permit conviction [38]. Federal and California laws have tight criminal statutes covering such entries, even if no damage is done [47]. In addition, civil law permits recovery not only of damages, but also of the costs to trace the culprit [6]. In practice, we found police agencies relatively uninterested until monetary loss could be quantified and damages demonstrated. Although not a substitute for competent legal advice, spending several days in law libraries researching both the statutes and precedents set in case law proved helpful. Since this case was international in scope, it was necessary to work closely with law-enforcement organizations in California, the FBI in the United States, and the BKA in Germany. Cooperation between system managers, communications technicians, and network operators was excellent. It proved more difficult to get bureaucratic organizations to communicate with one another as effectively. With many organizational boundaries crossed, including state, national, commercial, university, and military, there was confusion as to responsibility: Most organizations recognized the seriousness of these break-ins, yet no one agency had clear responsibility to solve it. A common response was, "That's an interesting problem, but it's not our bailiwick." Overcomimng this bureaucratic indifference was a continual problem. Our laboratory notebook proved useful in motivating organizations: When individuals saw the extent of the break-ins, they were able to explain them to their colleagues and take action. In addition, new criminal laws were enacted that more tightly defined what constituted a prosecutable offense [6, 38, 47]. As these new laws took effect, the FBI became much more interested in this case, finding statutory grounds for prosecution. The FBI and BKA maintained active investigations. Some subjects have been apprehended, but as yet the author does not know the extent to which they have been prosecuted. With recent laws and more skilled personnel, we can expect faster and more effective responses from law-enforcement agencies.

ERRORS AND PROBLEMS

In retrospect, we can point to many errors we made before and during these intrusions. Like other academic organizations, we had given little thought to securing our system, believing that standard vendor provisions were sufficient because nobody would be interested in us. Our scientists' research is entirely in the public domain, and many felt that security measures would only hinder their productivity. With increased connectivity, we had not examined our networks for crosslinks where an intruder might hide. These problems were exacerbated on our UNIX systems, which are used almost exclusively for mail and text processing, rather than for heavy computation. Password security under Berkeley UNIX is not optimal; it lacks password aging, expiration, and exclusion of passwords found in dictionaries. Moreover, UNIX password integrity depends solely on encryption; the password file is publicly readable. Other operating systems protect the password file with encryption, access controls, and alarms. We had not paid much attention to choosing good passwords (fully 20 percent of our users' passwords fell to a dictionary-based password cracker). Indeed, we had allowed our Tymnet password to become public, foolishly believing that the system log-in password should be our only line of defense. Once we detected the intruder, the first few days were confused, since nobody knew what our response ought to be. Our accounting files were misleading since the system clocks had been allowed to drift several minutes. Although our LAN's connections had been saved, nobody knew the file format, and it was frustrating to find that its clock had drifted by several hours. In short, we were unprepared to trace our LAN and had to learn quickly. We did not know who to contact in the law-enforcement community. At first, assuming that the intruder was local, our district attorney obtained the necessary warrants. Later, as we

learned that the intruder was out of state, we experienced frustration in getting federal law-enforcement support. Finally, after tracing the intruder abroad, we encountered a whole new set of ill-defined interfaces between organizations. The investigation stretched out far beyond our expectations. Naively expecting the problem to be solved by a series of phone traces, we were disappointed when the pathway proved to be a tangle of digital and analog connections. Without funding to carry out an investigation of this length, we were constantly tempted to drop it entirely. A number of minor problems bubbled up, which we were able to handle along the way. For a while this intruder's activity appeared similar to that of someone breaking into Stanford University; this confused our investigation for a short time. Keeping our work out of the news was difficult, especially because our staff is active in the computing world. Fortunately, it was possible to recover from the few leaks that occurred. At first, we were confused by not realizing the depth or extent of the penetrations. Our initial confusion gave way to an organized response as we made the proper contacts and began tracing the intruder. As pointed out by others [25, 36], advance preparations make all the difference.

LESSONS

As a case study, this investigation demonstrates several well-known points that lead to some knotty questions. Throughout this we are reminded that security is a human problem that cannot be solved by technical solutions alone [48]. The almost obsessive persistence of serious penetrators is astonishing. Once networked, our computers can be accessed via a tangle of connections from places we had never thought of. An intruder, limited only by patience, can attack from a variety of directions, searching for the weakest entry point. How can we analyze our systems' vulnerability in this environment? Who is responsible for network security? The network builder? The managers of the end nodes? The network users? The security weaknesses of both systems and networks, particularly the needless vulnerability due to sloppy systems management and administration, result in a surprising success rate for unsophisticated attacks. How are we to educate our users, system managers, and administrators? Social, ethical, and legal problems abound. How do we measure the harm done by these penetrators? By files deleted or by time wasted? By information copied? If no files are corrupted, but information is copied, what damage has been done? What constitutes unreasonable behavior on a network? Attempting to illicitly log in to a foreign computer? Inquiring who is currently logged in there? Exporting a file mistakenly made world readable? Exploiting an unpatched hole in another's system? Closing out an intruder upon discovery may be a premature reflex. Determining the extent of the damage and cooperating with investigations argue for leaving the system open. How do we balance the possible benefits of tracking an intruder against the risks of damage or embarrassment? Our technique of catching an intruder by providing bait and then watching what got nibbled is little more than catching flies with honey. It can be easily extended to determine intruders' interests by presenting them with a variety of possible subjects (games, financial data, academic gossip, military news). Setting up alarmed files is straightforward, so this mechanism offers a method to both detect and classify intruders. It should not be used indiscriminately, however. Files with plaintext passwords are common in remote job entry computers, yet these systems often are not protected since they have little computational capability. Such systems are usually widely networked, allowing entry from many sources. These computers are fertile grounds for password theft through file scavenging since the passwords are left in easily read command procedures. These files also contain instructions

to make the network connection. Random character passwords make this problem worse, since users not wishing to memorize them are more likely to write such passwords into files. How can we make secure remote procedure calls and remote batch job submissions? Passwords are at the heart of computer security. Requirements for a quality password are few: Passwords must be nonguessable, not in a dictionary, changed every few months, and easily remembered. User-generated passwords usually fail to meet the first three criteria, and machine-generated passwords fail the last. Several compromises exist: forcing "pass phrases" or any password that contains a special character. There are many other possibilities, but none are implemented widely. The Department of Defense recommends pronounceable machine-generated words or pass phrases [5]. Despite such obvious rules, we (and the intruder) found that poor-quality passwords pervaded our networked communities. How can we make users choose good passwords? Should we? Vendors usually distribute weakly protected systems software, relying on the installer to enable protections and disable default accounts. Installers often do not care, and system managers inherit these weak systems. Today, the majority of computer users are naive; they install systems the way the manufacturer suggests or simply unpackage systems without checking. Vendors distribute systems with default accounts and backdoor entryways left over from software development. Since many customers buy computers based on capability rather than security, vendors seldom distribute secure software. It is easy to write procedures that warn of obvious insecurities, yet vendors are not supplying them. Capable, aware system managers with plenty of time do not need these tools--the tools are for novices who are likely to overlook obvious holes. When vendors do not see security as a selling point, how can we encourage them to distribute more secure systems? Patches to operating-system security holes are poorly publicized and spottily distributed. This seems to be due to the paranoia surrounding these discoveries, the thousands of systems without systems administrators, and the lack of channels to spread the news. Also, many security problems are specific to a single version of an operating system or require systems experience to understand. Together, these promote ignorance of problems, threats, and solutions. We need a central clearinghouse to receive reports of problems, analyze their importance, and disseminate trustworthy solutions. How can we inform people wearing white hats about security problems, while preventing evil people from learning or exploiting these holes? Perhaps zero-knowledge proofs [20] can play a part in this. Operating systems can record unsuccessful log ins. Of the hundreds of attempted log ins into computers attached to internet, only five sites (or 1-2 percent) contacted us when they detected an attempted break-in. Clearly, system managers are not watching for intruders, who might appear as neighbors, trying to sneak into their computers. Our networks are like communities or neighborhoods, and so we are surprised when we find unneighborly behavior. Does security interfere with operational demands? Some security measures, like random passwords or strict isolation, are indeed onerous and can be self-defeating. But many measures neither interfere with legitimate users nor reduce the system's capabilities. For example, expiring unused accounts hurts no one and is likely to free up disk space. Well thought out management techniques and effective security measures do not bother ordinary users, yet they shut out or detect intruders.

INTERNET SECURITY

The intruder's successes and failures provide a reasonable snapshot of overall security in the more than 20,000 computers connected to Internet. A more detailed analysis of these attacks is to be published in the Proceedings of the 11th National Computer Security Conference [43]. Of

the 450 attacked computers, half were unavailable when the intruder tried to connect to them. He tried to log into the 220 available computers with obvious account names and trivial passwords. Of these 220 attempted log ins, listed in increasing importance, * 5 percent were refused by a distant computer (set to reject LBL connects), * 82 percent failed on incorrect user name/passwords, * 8 percent gave information about the system status (who, sysstat, etc.), * 1 percent achieved limited access to databases or electronic-mail shells, * 2 percent yielded normal user privileges and a programming environment, and * 2 percent reached system-manager privileges. Most attempts were into MILNET computers (Defense Data Network address groups 26.i.j.k). Assuming the population is representative of nonmilitary computers and the last three categories represent successful penetrations, we find that about 5 percent of Internet computers are grossly insecure against trivial attacks. This figure is only a lower limit of vulnerability, since military computers may be expected to be more secure than civilian systems. Further, cleverer tactics for entering computers could well lead to many more break-ins. Whereas the commercial sector is more concerned with data integrity, the military worries about control of disclosure [8]. With this in mind, we expect greater success for the browser or data thief in the commercial world. In a different set of penetrations [37], NASA experienced about 130 break-ins into its nonclassified, academic computers on the SPAN networks. Both the NASA break-in and our set of intrusions originated in West Germany, using similar communications links and searching for "secret" information. Pending completion of law enforcement and prosecution, the author does not make conjectures as to the relationships between these different break-ins. Between 700 and 3000 computers are reachable on the SPAN network (exact figures depend on whether LANs are counted). In that incident the break-in success rate was between 4 and 20 percent. Considering the SPAN break-ins with the present study, we find that, depending on the methods chosen, break-in success rates of 3-20 percent may be expected in typical network environments.

CONCLUSIONS AND COMMENTS

Perhaps no computer or network can be totally secure. This study suggests that any operating system will be insecure when obvious security rules are ignored. From the intruder's widespread success, it appears that users, managers, and vendors routinely fail to use sound security practices. These problems are not limited to our site or the few dozen systems that we saw penetrated, but are networkwide. Lax system management makes patching utility software or tightening a few systems ineffective. We found this intruder to be a competent, patient programmer, experienced in several operating systems. Alas, some system managers violate their positions of trust and confidence. Our worldwide community of digital networks requires a sense of responsibility. Unfortunately, this is missing in some technically competent people. Some speak of a "hacker ethic" of not changing data [37]. It is astounding that intruders blithely tamper with someone else's operating system, never thinking they may destroy months of work by systems people, or may cause unforeseen system instabilities or crashes. Sadly, few realize the delicacy of the systems they fool with or the amount of systems staff time they waste. The foreign origin of the source, the military computers entered, and the keywords searched suggest international espionage. This author does not speculate as to whether this actually was espionage, but does not doubt that someone took the opportunity to try. Break-ins from abroad seem to be increasing. Probably this individual's intrusions are different from others only in that his efforts were noticed, monitored, and documented. LBL has detected other attempted intrusions from several European countries, as well as from the Orient. Individuals in Germany

[37] have claimed responsibility for breaking into foreign computers. Such braggadocio may impress an unenlightened public; it has a different effect on administrators trying to maintain and expand networks. Indeed, funding agencies have already eliminated some international links due to these concerns. Break-ins ultimately destroy the network connectivity they exploit. If this is the object of such groups as the German Chaos Club, Data Travellers, Network Rangers, or various contributors to 2600 Magazine, it reflects the self-destructive folly of their apparent cleverness. Tracking down espionage attempts over the digital networks may be the most dramatic aspect of this work. But it is more useful to realize that analytic research methods can be fruitfully applied to problems as bizarre as computer break-ins. It seems that everyone wants to hear stories about someone else's troubles, but few are willing to write about their own. We hope that in publishing this report we will encourage sound administrative practices. Vandals and other criminals reading this article will find a way to rationalize breaking into computers. This article cannot teach these people ethics; we can only hope to reach those who are unaware of these miscreants. An enterprising programmer can enter many computers, just as a capable burglar can break into many homes. It is an understandable response to lock the door, sever connections, and put up elaborate barriers. Perhaps this is necessary, but it saddens the author, who would rather see future networks and computer communities built on honesty and trust.

NEWS - DICAS - CARTAS

WWW POR EMAIL

(nome editado - ver creditos)

submeta informatica-jb, submeta internet, submeta www-jb

Todos (?) os servidores WWW via e-mail

Endereco	Sintaxe	Pais
w3mail@gmd.de	get URL	Alemanha
agora@dna.affrc.go.jp	send URL	Japao
agora@kamakura.mss.co.jp	send URL	Japao
agora@info.lanic.utexas.edu	send URL	EUA
www.mail@ciesin.org	send URL	EUA
web-mail@ebay.com	URL	EUA
agora@mx.nsu.nsk.su	send URL	Russia
w3mail@elvis.ru	get URL	Russia
webmail@www.ucc.ie	go URL	Irlanda

Envie uma mensagem formada so' pela palavra help para obter informacoes detalhadas a respeito de cada servidor. O que tem o melhor 'help' e' o servidor japones agora@dna.affrc.go.jp.

Todos esses servidores tem algumas falhas. Meu predileto e' o servidor alemao, mas so' neste ano ele ja' passou mais de 1 mes com problemas. Quase todos limitam os pedidos dos usuarios (por exemplo, no maximo a 5000 linhas de texto).

Os servidores da Russia foram acrescentados somente porque esta pequena lista tem a pretensao de ser completa. Os servidores russos atendem somente `a Russia.

Voce pode capturar via e-mail qualquer informacao contida em paginas da WWW. As imagens podem vir em varios formatos, por ex., no formato uuencode. Pesquisas no Alta Vista, Yahoo etc. tambem podem ser feitas usando-se esses servidores. Quando eles estao funcionando, sao sempre muito gentis e eficientes.

Exemplo 1: A seguinte mensagem pode ser enviada para o servidor Agora americano pedindo a ele para enviar gentilmente informacoes sobre uma pagina WWW de Recife:

```
To: agora@info.lanic.utexas.edu
Subject:
-----------------------------------------------
send http://www.elogica.com.br
send http://www.elogica.com.br/dicas/jorna.html
send http://www.elogica.com.br/dicas/portu.html
```

Exemplo 2: Envie a mensagem a seguir para o servidor alemao para obter algumas imagens da Grecia no formato uuencode (opcao -uu):

```
To: w3mail@gmd.de
Subject:
-------------------------------------------------------------
get -uu http://www.mechan.ntua.gr/webacropol/acropol.jpg
get -uu http://www.mechan.ntua.gr/webacropol/propylaia.jpg
get -uu http://www.mechan.ntua.gr/webacropol/parthenonas.jpg

--======================_838717622==_--
```

=-=-=-=-=-=-=-

NOTICIA OU DICA VELHA, MAS .. INTERESSANTE

Todo mundo ja' sabe que virus de computador existe. Alguns sabem ate' que existe tambem kits de construcao de virus de computador. Mas muito poucos sabem da existencia de laboratorios completos para a producao de virus. Tava segurando essa noticia por um tempo. Para ser exato, o lugar onde peguei esse arquivo nao existe mais. Parece que houve uma limpeza total na rede norte-americana. Paginas inteiras na web, dedicadas a hacking, como o Materva Hideout, estao ficando inacessiveis. Sacanagem eu divulgar so' agora a existencia desse negocio, mas tambem... eram cinco ou seis arquivos de mais de 1 megabyte. Talvez num proximo numero escrevo sobre isso.
Detalhe: Existe uma lista de virus na esquina-das-listas
Deve haver alguem no Brasil q. tem esses arquivos. Nao procurem a mim p. informacoes. Ja' basta a perseguicao q. enfrento por editar um zine para hackers. To com medo ate' de ir p. os EUA. Fico pe^ da vida com a sugestao de enviar virus pela rede.

----------README 1ST DE UM LABORATORIO DE VIRUS----------
(NAO ME PERGUNTE ONDE ACHAR - SO' COLOQUEI A TITULO DE INFORMACAO)

O R I G I N A L R E L E A S E

Viral Collector's Kit #1

By

The Knights of Chaos

Released into the world on 02/04/95

This is a Knights of Chaos Original Release. We've compiled this large package of 270 viruses, virus creating and writing tools, informational text files and Virus Group Magazines, and brought them together into VCK #1.

We plan on releasing 1000+ viruses total in sequel Viral Collector's Kits.

The Viruses you'll find in this package are documented and BBS ready. What does that mean? They've been pre file_id.diz'ed with the virus' common name and the name it can be found under in Patricia Hoffman's Virus Summary (VSUMX 4.1). Each zip is pre-loaded with a warning disclaimer about the contents, an excerpt from VSUMX 4.1 about what the virus is and what it does. All you have to do is put them up on your board if you support virus transfers.

Our main goal is to provide many computer viruses for reverse engineering for those who are curious about how viruses work. Many virus source code files are also included.

What you get in Viral Collector's Kit #1

You Get:

Virus Tools and Files

* 270 Viruses in our Numerical, A, B, and C Groups
  (BBS Ready! Pre file_id.diz'd)
* Nowhere Man's Virus Construction Lab
* Mad Maniac's Mutation Engine for Polymorphic Viruses
* Dark Slayer's Confusion Engine for Polymorphic Viruses
* GenVirus Construction Lab (French)
* KOH, An encryption virus for keeping your data secret
* 9 virus ASM files by Immortal Riot

Programs and Disassembling Tools

* A86 v4.00 Macro Assembler (Shareware)
* D86 v4.00 Debugger (Shareware)
* Disaster v1.0 Disassembler (Shareware)
* ASM Editor Three (Shareware)
* Nowhere Man's NowhereUtilities
* Detector, A Virus Strain detector
* CatDiz, A File_id.diz cataloging system (Freeware)
* Dizview, View Diz files within Zip Files (Shareware)
* UUENCODE & UUDECODE for sending us files via internet

Virus Scanners and Virus Signature Update Files

* VSUMX v4.10 Virus Summary Hypertext (Shareware)
* McAfee Scan v2.14E (Shareware)
* Latest Central Point Anti-Virus 2.x Signature Updates

    For Dos and Windows released 01/06/95
  * ThunderByte Anti-Virus v6.31 with processor optimized EXE
    files.

  Informational Texts and 'Zines

  * Skism's 40Hex Magazine Issues 1 through 13
  * Phalcon/Skism's Virus Texts 1 through 5
  * Crypt Newsletter Issues 1 through 29 (missing issues)
  * NuKE InfoJournals 1 through 8

  Miscellaneous

  * Knights of Chaos' PGP Public Key
  * K-RaD README and VCK-1 Hypertexted files (Be sure to read them!)

Have Fun!

Neural Nightmare/K.Chaos '95

Computer Attacks On Pentagon Growing, Report Says

WASHINGTON (May 23, 1996 00:11 a.m. EDT) -- There may be as many as 250,000 attacks on Pentagon computer systems every year and "the potential for catastrophic damage is great," a government report said today.

The General Accounting Office of Congress said hacker attacks on Pentagon computer programs are successful some 65 percent of the time, and the number of attacks is doubling every year.

"These so-called hacker intrusions not only cost Defense tens of millions of dollars, but pose a serious threat to our national security," said Jack Brock, the information management director of GAO, the investigative office of Congress.

The report, based on Pentagon estimates, was submitted to the Senate Governmental Affairs subcommittee on investigations.

Sen. Sam Nunn of Georgia, ranking Democrat on the panel, said cyberspace crime poses a whole new challenge to the government. "Is the bad actor a 16-year old, a foreign agent, an anarchist or a combination thereof?" he asked. "How do you ascertain the nature of a threat if you don't know the motive of your adversary?"

Brock described the case of a 16-year-old British youth who in 1994 broke into the computer of the Air Force command and control research facility in Rome, New York. The youth gained access to the system more than 150 times by weaving through international phone systems in South America, Seattle and New York.

The youth also used the Rome lab computer systems to gain access to systems at NASA's space flight center, defense contractors around the country and the South Korean atomic energy center. A second hacker who was making similar penetrations of the system was never caught.

The hackers had access to orders military commanders send during wartime to pilots with information on air battle tactics.

Brock said that if the research project at Rome had been damaged beyond repair, it would have cost about $4 million and three years to replace it.

With the explosion of use of the Internet, originally established for military communication, there are some 40 million computers around the world with the potential to search for the more than 90 percent of Pentagon computer files that are unclassified. "Every node is a potential spy," said Keith Rhodes, the GAO's technical assistance director.

The report said also noted that some 120 governments around the world have or are developing computer attack capabilities.

It recommended that the Pentagon work for a greater degree of computer file accountability, institute rigorous training in computer security and develop better capability for reacting to break-ins.

[Copyright) 1996 Nando.net]
[Copyright) 1996 The Associated Press]

Subject: pgp..

Oi, gente,

> PARA DISCUSSAO NA LISTA INTERNET
>
> =20
> Paulo Rubem Santiago
>
>
>
>
>>Quebra de sigilo na Internet-BR
>>
>>Em breve, a policia no Brasil podera ler suas mensagens de e-mail sem
>>que voc=EA saiba. No dia 24 de julho, o presidente Fernando Henrique
>>Cardoso sancionou a lei 9.296/96, que entre outras coisas, permite a
>>interceptacao de comunicacoes realizadas via computador.
>
>
>Porque o e-mail esta' sendo devassado assim indiscriminadamente, quando o
>telefone e a conta bancaria tem leis bem rigidas para que se autorize a
devassa?
>
>
>
>
>>A lei regulamenta o monitoramento e interceptacao para prova em
>>investigacao criminal de comunicacoes telefonicas de qualquer natureza.
>>Isso significa que, nao so a sua caixa de correio eletronico esta
>>ameacada, mas e' possivel que a policia, durante uma investigacao, faca
>>escuta no seu telefone, fax, sessao de chat ou postagem em foruns e
>>grupos de discussao.
>>=C9 preciso autorizacao judicial para realizar a escuta, mas o pedido
pode
>>ser formulado verbalmente, desde que sejam apresentadas as
>>justificativas. Determina a lei que a policia podera requisitar ajuda de
>>te'cnicos das empresas operadoras de servicos de telecomunicacoes.

A
>>gravacao que nao servir como prova sera destruida na presenca do
>>acusado ou seu representante legal.
>>

Concordo que o e' um absurdo que nossas mensagens e comunicacoes
digitais tenham esse tipo de tratamento, de poderem ser interceptadas
sem necessidade de mandado judicial. Honestamente nao li o texto da lei
em questao, e tambem nao sou expert em leis, mas vou pesquisar melhor.

Entretanto, existem solucoes tecnologicas. Por exemplo, o PGP e' um excelente
programa de criptografia que torna suas mensagens de correio eletronico vir-
tualmente indecifraveis, e quanto a isso nao tem Policia Federal nem Govern
o
Brasileiro que possa fazer absolutamente nada. De fato, a criptografia do
PGP e' tao forte que ate' o Governo dos EUA -- especialmente a National Sec=
urity
Agency -- tentou processar o autor do programa e bani-lo da Internet. Ambas
as tentativas nao tiveram sucesso.

Eu pessoalmente uso o PGP ha' varios anos para minhas comunicacoes privativas.
Entao, a lei do FHC que venha. Podem ate' me interceptar, mas nao vao poder
entender bulhufas, mesmo. ;)

Recentemente o autor do PGP, o Phillip Zimmermann, criou o PGPFone, que e'um
programa de conversa via voz em tempo real na Internet, `a la Internet Phon
e,
que usa os mesmos recursos de criptografia. Ainda nao vi, mas parece ser
legal.

Autoria: Question Mark

Continuando a mensagem anterior....

Subject: mais pgp

Caros colegas

Parece-me que a nova legislacao tem raizes bem mais antigas.
Senao ,vejamos:
Em certo ponto de um dos arquivos texto que acham-se incluidos
no PGP(vide Pgpdoc1.txt e Pgpdoc2.txt),o Sr.Zimmermann,autor desse
programa de criptografia,tece varias consideracoes sobre tentativas
de criacao de censura levadas a efeito:
- pelo Senado dos Estados Unidos(projeto de lei 266,1991)o qual,
se aprovado, forcaria os fabricantes de equipamentos de seguranca
em comunicacoes a inserir armadilhas (trap doors) especiais em
seus produtos de modo a que o Governo pudesse ler as mensagens
criptografadas ,quando autorizado por lei. Textualmente:
"It is the sense of Congress that providers of electronic
communications services and manufacturers of electronic
communications service equipment shall insure that communications
systems permit the Government to obtain the plain text contents
of voice,data and other communications when appropriately
authorized by law ."
Este Projeto foi derrotado face aos rigorosos protestos de grupos
partidarios da doutrina do livre arbitrio e tambem de grupos

industriais.
- pelo "FBI Digital Telephony " que enviou ao Congresso (1992)proposta visando a aprovacao de "grampeamento " ("wiretaps").
  Esta proposta requereria a todos os fabricantes de equipamentos de comunicacoes que instalassem portas especiais de grampeamento remoto as quais possibilitariam ao FBI grampear, remotamente, todas as formas de comunicacoes a partir de seus escritorios.
  Esta proposta,ainda que nao tenha atraido quaisquer patrocinadores no Congrasso face a oposicao dos cidadaos,foi reintroduzida em 1994.
- e,a mais alarmante de todas,pela sugestao da Casa Branca de uma nova politica sobre criptografia ,em fase de desenvolvimento pela NSA desde o inicio da administracao de Bush, revelada em 16 de abril de 1993.O ponto central dessa sugestao e um dispositivo de codificacao,denominado circuito integrado "Clipper", construido pelo Governo,contendo um novo algoritmo secreto de criptografia desenvolvido pela NSA.O Governo esta encorajando a industria privada a projeta-lo em todos os seus produtos de comunicacao de seguranca como fones,Fax etc. AT&T esta agora colocando o Clipper em seus produtos de voz.A armadilha:Quando por ocasiao da fabricacao cada circuito Clipper seria carregado com sua chave unica,da qual o Governo receberia uma copia.Nada preocupante nao obstante o Governo prometer que somente usaria estas chaves quando autorizado por lei.Naturalmente ,para tornar o Clipper completamente efetivo, o proximo passo logico seria tornar ilegal outras formas de criptografia.

Conclue entao o Sr.Zimmerman que : Se a privacidade for tornada ilegal, somente os "fora-da-lei" terao privacidade.Os Servicos Secretos tem acesso a boa tecnologia criptografica.O mesmo sucede aos grandes traficantes de armas e de drogas bem como as Companhias de Petroleo e outras corporacoes gigantescas.

Enquanto isso as pessoas comuns nao tem acesso a tais tecnologias criptograficas de chave publica.

Ate agora nao tinham,finaliza o Sr.Zimmerman,visto que o PGP fornece a estas pessoas o poder de manter sua privacidade em suas proprias maos. Este o motivo pelo qual eu escrevi o PGP,afirma.

Torna-se para mim evidente a ingenuidade de leis que pretendem fiscalizar os e-mail dos componentes da WWW.
Isto por varios motivos:

1-Somente um louco iria confiar a uma simples senha de e-mail quaisquer assuntos ilegais.Essas senhas sao de uma fragilidade espantosa.Nem ha necessidade de sistemas sofisticados para descobri-las.
Quem duvidar experimente ver a simplicidade do algoritmo utilizado pelo WS-FTP no arquivo WS-ftp.ini,onde sua senha de e-mail fica codificada em hexadecimal.

2-A quantidade astronomica de mensagens que circulam pelas provedoras tornaria o processo absolutamente inviavel,pelo menos economicamente.Basta que voces vejam o que sucede na elogica/noticias-l e outras: algo em torno de 60 a 70 mensagens por dia.E evidente que haveria que fiscalizar tambem as mensagens provenientes do exterior.E ha mais de 50 milhoes de usuarios no mundo,segundo dizem.

3-E que dizer de pessoas que declaram, pela midia,terem acertado mais de duzentas vezes nas diversas loterias.
Notar que elas nem usavam e-mail !!!
E,segundo parece,torna-se muito dificil fiscaliza-las.
Observar que qualquer semelhanca com pessoas ou fatos reais tera sido mera coincidencia.

Envio a todos as minhas desculpas pela extensao do texto .

Ass: Question Mark

Objetivos Comitjs e eleigco HomePage Ranking ANUI Concurso de logos
Livro de Inscrigues links

ASSINE O ABAIXO-ASSINADO
PELA REVOGAGCO DA LEI QUE DEVASSA O E-MAIL!

Quebra de sigilo na Internet-BR

Em breve, a polmcia no Brasil podera ler suas mensagens de e-mail sem que vocj saiba. No dia 24 de julho, o presidente Fernando Henrique Cardoso sancionou a lei 9.296/96, que entre outras coisas, permite a interceptagco de comunicagues realizadas via computador.
A lei regulamenta o monitoramento e interceptagco para prova em investigagco criminal de comunicagues teleftnicas de qualquer natureza. Isso significa que, nco ss a sua caixa de correio eletrtnico esta ameagada, mas i possmvel que a polmcia, durante uma investigagco, faga escuta no seu telefone, fax, sessco de chat ou postagem em fsruns e grupos de discussco.
I preciso autorizagco judicial para realizar a escuta, mas o pedido pode ser formulado verbalmente, desde que sejam apresentadas as justificativas. Determina a lei que a polmcia podera requisitar ajuda de ticnicos das empresas operadoras de servigos de telecomunicagues. A gravagco que nco servir como prova sera destrumda na presenga do acusado ou seu representante legal.

MOVIMENTOS QUE ESTAO NA LUTA CONTRA ESSA MEDIDA:

Aqui no Brasil:

Movimento Li-br-dade da Micheline
http://webcom.com/lalo/li-br-dade.html

Tema da Hora.
http://www.bol.com.br/cult/tema

ANUI - Associagco Nacional dos Usuarios da Internet
http://www.cinemabrazil.com/ANUI.br

No exterior:

Espanha:
Associacion de los Usuarios de Internet - AUI
href=http://www.aui.es/

Franga:
Association de Utilizateurs de Internet - AUI
http://www.aui.fr/

From: "Midia Eletron. e Criacao Artistica"

submeta musica internet cinema www-jb

Esta' no ar o numero 1 da revista eletronica Zambo Zine, no endereco:

http://medusa.ufscar.br/Portugues/Centros/CECH/DArtes/index.htm

Neste numero:

-Straight Edge, Shelter, punk rock

-Cinema: Cassiopeia

-Musica: progressivo, Spacehog

- e muito mais!

Nao deixe de visitar!
Opinioes, sugestoes e criticas serao benvindas.

Thiago Baraldi
zine@iris.ufscar.br

From: ????? ??????
Subject: mais conteudo!!!
Status: RO
X-Status: A

Gosto da Barata eletrica, mas falta conteudo underground, tem muitas historias e causos mas esta faltando
algo mais.... passe a publica-la via listas preivadas ou coisa assim, sei muito pouco de unix, mas conheco
sei o valor da informacao. vamos procurar tratar disto de forma mais agressiva.

me escreva em ????????@??????.????br

RESPOSTA: O motivo da minha timidez e' uma lei, a 5250 de 9/2/67 Codigo Penal. Capitulo III artigo 19 - incitar a pratica de infracoes penais. Tem outras leis, relativas a revelacao de dados confidenciais das forcas armadas e uma outra que proibe denegrir a imagem de orgaos publicos. Tem lei pra tudo. Prefiro nao facilitar.

DICAS PARA WANNA-BEs

submeta hackers

Vou dar uma "dica" a voces.

1o - Escolha um nick (apelido)
2o - Procure saber do que voce esta conversando ou falando
3o - Nunca se julgue o tal - "aquele que e bom sera reconhecido"
4o - Quando ver algo que vc sabe opine sobre

5o - Ajude os outros
E isso.
Regards,
K00Li0

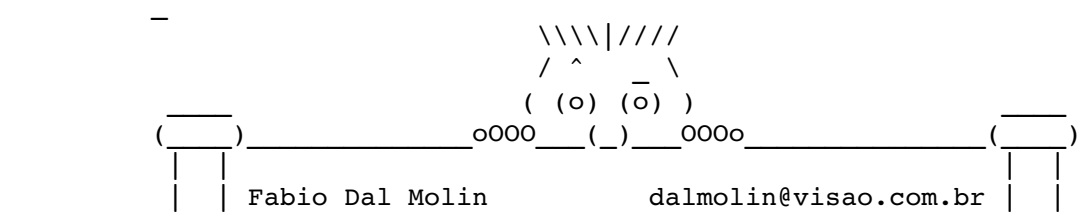
---

submeta hackers

Quem estiver interessado em entrar no grupo de hackers que estamos formando, mande um mail para dalmolin@visao.com.br e "add hackers" no corpo. Seu e-mail sera' automaticamente inscrito em uma lista de distribuicao. E' um comeco. :)

Temos que escolher um nome legal, eu nao tenho ideia, mas mandem suas sugestoes para a lista hackers. Depois eu mando uma copia do arquivo da lista de distribuicao (pegasus mail) para quem for o organizador do grupo.

[]'s Fabio.



GRUPO DE HACKER

Venho por meio desta informar a todos os interessados
em formar grupo de hackers, que aqui em Porto Alegre ja
ocorreu o primeiro encontro.
E convido a todos q residem aqui em POA a participar
(interessados mandar e-mail p/ o meu endereco mboth@plug-in.com.br)
e os q nao residem a nos encontrar em um canal de IRC.
irc.kanopus.com.br - port. 6667 e canal "GHBR" ((Group the
Hacker from Brazil) um nome discreto para nao "entupir" de gente.
o dia e horario esta ainda para ser definido.

Aguardo sugestao de todos.
Aguardem novas mensagens...

Abraco MBoth

O TIPO DE CARTA QUE NAO RESPONDO

Volta e meia, gente me escreve umas cartas desse tipo. Nao e' ma' vontade, mas nao vou ensinar esse tipo de coisa, principalmente por correio eletronico. Eu ja' me exponho pra caramba escrevendo este fanzine vou me expor ainda mais ensinando contravencao? Quando vejo este tipo de carta, pensamentos tao infelizes me ocorrem... ou o leitor e' um gozador tirando sarro da minha cara, ou e' alguem que acabou de ler dois artigos e acha que pode perguntar que "eu dou o servico". Ja' sao cerca de 37, o numero de pessoas que ja' escreveram cartas iguais a que esta' abaixo. Eu nao estou procurando aprendizes p. ensinar minha arte. E nao acredito em mestres. Provavelmente, o tipo de aula que ja' pensei em dar nao seria gratuito como o Barata Eletrica e nao abrangeria contravencao do tipo dar o cano na telefonica. Aqueles q. esperam dicas sobre como e' que se assalta

um banco, qual o codigo xy que usa no banco ccc que tenham do' de mim. Nao sei. E' crime, nao vou ensinar.

Subject: BB

Ola Derneval,

Vc tem ai o BB (blue beep), sabe como usa-lo ou tem algum outro???

Eu tenho o Blue Box, mas nao funciona.

Peguei a BE do 0 a 11, super legal!!!! Parabens!!!!!!! :-D

[]'s Ffff

Subject: Bancos

E para conseguir senhas bancarias, tipo Bradesco Net
(www.bradesco.com.br), Banrisul (RENPAC), etc..
Vc sabe como fazer movimentacoes financeiras?????

Vc sabe como trocar o IP???? E quanto a IRC, vc sabe como pegar op sem lhe passarem, derrubar pessoas, entrar em canais secretos, dicar invisivel, etc..????

E vc sabe como pegar a senha de servidores FTP??

Parabens pela Barata Eletrica.

[]'s FFFF

Subject: Celular

Estou para comprar um aparelho celular, qual vc me aconselha para fazer escutas??

Tenho um bloqueador para chamadas interurbanas aqui em casa, como posso fazer para desativa-lo????
Uma vez consegui largando 220 volts na linha telefonica, queimou a central da cidade inteira, ficamos +d uma semana sem telefone.
Preciso de um jeito para desativar o bloqueador sem danos, tipo descobrir a senha dele, dar curto nele mas sem por a linha abaixo, etc.. :)

Vc sabe de algum meio de pegar senhas de usuarios via FTP ou outro meio??

E os credit card generators, o que fazem??
E' possivel pegar as senhas, nomes, validades, de outras pessoas para serem usadas para compras via Internet, etc..??

[]'s FFFFF

DIRETO DA LISTA HACKERS

submeta hackers
 >
 -=> Quoting ???? ?? ???????? ??????? to ????? ????????? <=-
 >
  ta bom! no confronto direto eu perdi. mas deixa eu explicar melhor

porque tem gente olhando e vai ficar chato se eu nao reagir. nao e'
nenhuma briga pessoal, mas e' uma questao de orgulho bobo, que me
obriga a esclarecer algumas coisinhas. la vou eu, com uma mensagem
em duas partes pra poder falar tudo o que eu preciso:
>
JDCF> ja' que eu tou atoa mesmo vou responder o questionario!! :)
valeu!
>
> * legal! o que queremos com o grupo de hackers?
> (   ) aprender a programar
JDCF> melhor comprar um livro... ou fazer um curso...
concordo.
>
> (   ) desenvolver grandes poderes porque programar eu ja sei
JDCF> melhor falar com a liga da justica...
bom eu sei que voce entendeu o que eu quiz dizer, mas a proposta
ainda ta de pe: quem quizer falar sobre programacao de rotinas
basicas de hardware (tipo acessar SB16, video...), estamos aqui
pra ajudar e aprender...
>
> (   ) exterminar com alguem
JDCF> usa detefon...
e' serio! quem souber exterminar com alguem e nao quizer me mostrar
do pior jeito, eu queria aprender...
>
> (   ) fazer projetos em prol do Grupo de Hacker$
>   (compra/venda/calambacho)
> (   ) colocar informacoes secretas empublico so pra variar
JDCF> e onde c vai arrumar informacoes secretas no brasil??? so se for
JDCF> conta bancaria de pulitico ladrao... mas ai ele da' um jeito de
JDCF> se safar... todos conseguem se safar... ate' PC saiu a francesa
pois e', mas quem disse que teria que ser daqui? pode ser umas coisas
classicas e basicas como entrar na NASA, disparar misseis nucleares no
oriente medio e acabar com o suprimento mundial de combustivel...
>
> (   ) fazer programas poderosos pra vender sob uma marca nossa
JDCF> essa ideia e' boa... afinal eu tou formando pra isso mesmo... :)
LEGAL !!! ate que enfim eu concordo com sua opiniao. se e' pra usar
o computador, porque nao conseguir dinheiro com ele? juntos entao?
>
> (   ) provar que o gates nao ta com nada e o ruindows
>   paga um p*u pro OS/2
JDCF> isso o proprio bill gates ja' fez... nao precisa fazer...
LEGAL II concordo de novo!
>
> (   ) provar que o gates e' o nerd master e que devemos tudo a ele
>
JDCF> que tal: (   ) transformar a lista de hackers em um grande chat
JDCF> parecido com o irc onde todo mundo interessantemente tem
JDCF> um delay de +- 24 horas??? afinal nao ta virando isso???
e esta mesmo. fazer o que? desafiar os verdadeiros hackerz poderosos
pra apagar nossas mensagens indefesas antes de podermos le-las? nao!
>
JDCF> [snip]
> * pra responder este segundo questionario, use valores de 0 a 10.
>
JDCF> *** comentario significativo: quem sabe programar programa em
JDCF> qualquer linguagem (ate' em LISP!!!) as limitacoes vem da
JDCF> linguagem e nao do programador.
esta e' parte da verdade. as linguagens podem sim limitar o

programador, mas so depende do programador - e e' isso que o
diferencia do usuario - tomar os caminhos necessarios para contornar
as dificuldades. a graca esta exatamente ai, cair no assembler baixo
nivel pra conseguir o que voce nao tem prontinho e mastigado
(leia-se VBX/DLL/LIB/OBJ/TPU...)
>
> (10) Linguagem C/C++
> (6) Java (e alguem pegou o Java Developement Kit ??? [CESAR])
> (9) Pascal / ObjectPascal / Delphi
> (0) Clipper (so que hacker nao programa em clipper [CESAR])
> (15) Visual Basic (VB e' coisa de crianca ne gente... [JDCF])
> (8) Assembler
> (7) Unix (eu nao sei [CESAR]) (csh, sh, awk e um tiquim de perl)
> (?) outros (como eu dou nota pra outros????[JDCF])
          ^^^^^^ diz em qual mais e da a nota poxa!!!
>
> ( ) quem chegou agora no mundo dos PCs (porque juro que nunca soube
> de hacker que usasse MAC, nao que nao possa, mas que nao apareceu
> ate hoje nao apareceu...), que acha o Windows o maximo com todas
> aquelas figuras coloridas
JDCF> mal informado tio... da uma lida em phrack, 2600, wired, etc...
JDCF> maioria Mac.
eu concordo que estou *BEM* por fora, entao se tiver jeito, me passa
uns links, diz nomes de revistas, e' que eu cheguei na net faz
pouco tempo...
>
> (X) quem veio do mundo do basic, e' mais o DOS que o ruindows,
> mas que admite que a interface grafica tem suas vantagens (eu!)
JDCF> ainda nao surgiu melhor alianca entre um e outro que X11 (unix
JDCF> x-windows)
nao conheco nao. parece que voce gosta mesmo do unix. voce trabalha
com ele? sabe onde aprender sem ser em faculdade? nao e' pra mim,
mas tenho uns amigos malucos que querem aprender...
>
> (X) quem prefere o OS/2 ao Windows 95
(eu! mas eu ainda estou no DOS) [CESAR]
JDCF> mas acho que unix e' bem melhor!!!
(humf...)
>
> (   ) quem prefere o Windows 95 ao OS/2
> (   ) quem e' hacker superpoderoso e que pode exterminar com todos
>   nos atraves de e-mail bomba, *MAS QUE ESTA DISPOSTO A
>   ENSINAR*
JDCF> e-mail bomba??? nan... ta' demode' demais...
JDCF> ate' os zapatistas ja'fizeram...
e voce sabe ensinar? eu queria aprender!
>
> (   ) quem programa legal, mas nao tem nenhum superpoder (eu!)
JDCF> que tal: (   ) tem interesse em seguranca de computadores e e'
JDCF> um agente infiltrado em grupos de hackers pra saber o quanto
JDCF> esses idiotas estao pra traz nesses assuntos e quanta grana a
JDCF> gente pode economizar diminuindo a seguranca do nosso sistema!
JDCF> porque nao? fica ai' mais uma proposta...
>
> * ta bom. pra concluir, deixa eu dizer o que eu quero com tudo isso.
> eu sou um cara normal (mesmo considerando que eu ate sei programar o
> videocassete), que programa legal, mas nao tem nenhum superpoder.
JDCF> ^^^^^^^^^^^
JDCF> ei... de que marca??? me da umas dicas cara.... e' serio... :)
video e' comigo mesmo. nao tem erro. so temos eu e o meu irmao que

sabemos usar o video aqui em casa. somos uns dos poucos no mundo
que sabemos fazer isso!
>
fim da parte I. leia a proxima :)

: HACKERS

---

submeta hackers
mensagem continuacao 2/2. procure a outra se voce perdeu o comeco...

> eu adoro *PASCAL*, e programo em C, Basic (e VB), Cobol, Asm, voceis
JDCF> tadim... PASCOAL!!! ou.. ce ta mais pra fazedor de programa de
JDCF> locadora que pra hacker viu!!!
ahh! nao e' bem assim! pascal tem tanto poder quanto C, mas e' mais
facil pro programador que pro compilador, e outra, nao e' todo
programador de pascal que faz coisas bestas nao, pascal e' perfeito
pra se aplicar teorias novas sem esforco. pode ver, fractais,
simulacao de fogo, manipulacao de memoria de video direto, e' muito
mais facil e rapido fazer em pascal,
mesmo que voce caia em assembler...
>
> sabem, fora pascal, eu dou meus chutes... [CESAR]
>
JDCF> tirando o knuth todo mundo da' seus chutes. (ate' o ricardo
JDCF> baesa-Yates e o wirth... e pelo visto o mitnick tambem ne'? :))
>
> e eu estou a fim de *APRENDER* e ensinar e' claro. mas eu queria
> formar um grupo de amigos (amigos mesmo! sem esse lance de ofender
> os outros por pouca coisa) que quisesse programar junto, sempre
> programas legais
>
JDCF> sem crise... nao se ofenda com minha gozacao do pascal...
entao ta legal.
>
> tecnicamente (tipo demos, cracks, source codes de tudo que for
> jeito), mas que nos fizessemos e passassemos pros outros. eu gosto
> de rotininhas assembler pra tocar sons, mostrar imagens, etc.
> e' meio baixo nivel, mas
>
JDCF> eu ja' gosto mais de rotininhas em "shell" pra pegar
JDCF> acesso de root... mas e' uma outra estoria...
entao conta ela pra nos! as vezes tem quem goste de aprender... :)
>
> e' aqui que esta a graca. nao de VBX ou OCX ou DLL ou TPU
> ou LIB ou OBJ, tudo source code free public domain, sem peso na
> consciencia.
JDCF> perai... e a gente faz dinheiro como???
JDCF> vendendo ingresso pro show dos mamonas???
opa! espera ai! voce nao entendeu! source code entre nos! ta bom que
na internet *entre nos* e' meio fora de questao, mas e' aqui onde
ficam as informacoes nao e'? nos usamos os sources pra fazer os
programas e vende-los, e nao o source code!
e' como o office da lixosoft: tem o VBA (visual basic for

applications) so' que nenhum usuario comum perderia seu tempo pra
fazer um controle de estoque no excel/access. essa e' a nossa parte
e entao eles compram e acham o maximo porque e' pra ruindows....
>
> * e' isso que eu tinha pra dizer. a mensagem ficou grande mas
> tinha que ficar claro. agora voces decidem que rumo levar.
> talvez ate criar mais um item na lista, tipo Grupo de Hackerz...
> imagina que legal: submeta grupo-de-hackerz
> (e mexa com a morte!!!)
JDCF> putz!!! ja nao basta ter de digitar esquina-das-listas toda
JDCF> vez inda vou ter que digitar
JDCF> grupo-de-hackers-e-mexa-com-a-morte ???
JDCF> acho que vou criar um alias...
naaaaooo! o mexa com a morte era um comentario meu! nao faz parte
do nome da lista!!!
>
> respondam entao. vamos agitar!!!
JDCF> beleza... encontro 2600 toda sexta feira as 16:30 na assufemg.
JDCF> (quem for um bom fucador descobre onde e')
eu fiquei boiando. que puder me explicar, por favor [CESAR]
>
>
> .. Sexta-Feira 13 parte CXXXVIII - Jason encontra a Enterprise
>
JDCF> falar nisso: alguem tem o texto "enterprise and windows" que
JDCF> circulou na net um tempo atraz??? to pricisando... eu so'
JDCF> tenho em papel...
>
>
JDCF> girino.
CONCLUSAO FINAL PARTE II:
poxa cara! voce deu um trabalhao e a mensagem ficou imensa!
mas ta legal. da proxima quem sabe agente concorda em mais alguma
coisa? vamos tentar.
>

BIBLIOGRAFIA:

O guerra eletronica foi feito com base no livro cujo titulo esta' no artigo e com leituras feitas alhures. O clipping veio do EDUPAGE, nada de novo.

O artigo sobre PGP foi feito com base na documentacao fornecida pelo software e experiencia pessoal.

O "Direito no Ciberespaco" foi enviado pelo autor e como ja' foi colocado, teria sido publicado numa revista juridica. Sinto nao ter usado a versao mais atual, essa era p. ter sido um rascunho. Faltou tempo e disposicao p. procurar o autor e conseguir a atualizacao.

Outros artigos vieram de fontes na rede ou enviados por amigos.