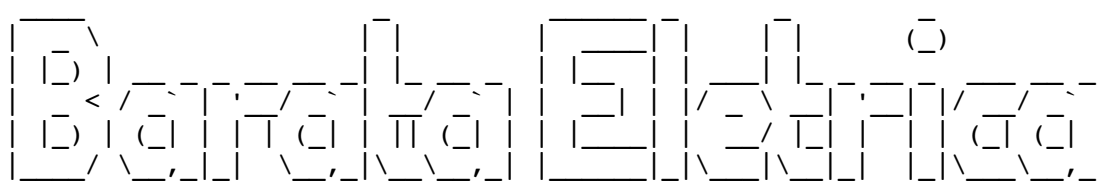

BARATA ELETRICA, numero 11
Sao Paulo, 8 de julho, 1996

Creditos:

Este jornal foi escrito por Derneval R. R. da Cunha
(wu100@fim.uni-erlangen.de - http://www.geocities.com/SiliconValley/5620)
Com as devidas excecoes, toda a redacao e' minha. Esta' liberada a copia (obvio) em formato eletronico, mas se trechos forem usados em outras publicacoes, por favor incluam de onde tiraram e quem escreveu.

DISTRIBUICAO LIBERADA PARA TODOS, desde que mantido o copyright e a gratuidade. O E-zine e' gratis e nao pode ser vendido (senao vou querer minha parte).

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

rodrigde@spider.usp.br

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 9):

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
patrick@summer.com.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
INDICE
HACKERS: O FILME E A VIDA REAL
UNIX - MELHOR QUE WINDOWS 95?
COMO ESCONDER SEUS DADOS, VALORES E SEGREDOS
BBSES QUE NAO ESTAO NO MAPA
STALKING THE WILY HACKER
PERGUNTAS MAIS FREQUENTES SOBRE "ANONYMOUS REMAILERS"
DIARIO DE UM USUARIO AOL (HUMOR)
MURPHOLOGIA AVANCADA
CARTAS - DICAS - NOVIDADES
BIBLIOGRAFIA

E ai', gente? Mais um Barata Eletrica. E', como a USP ta' de greve, varias coisas pintando, realmente to conseguindo botar uma producao menos espacada. Tem gente ajudando, tambem. E .. sai de novo na imprensa: na revista HomePC. Pra variar, materia sobre o Mitnick. Mas tudo bem. Montei um contador na minha Web-page (ver abaixo) e ja' alcancei os 480 acessos. Nada mal. To escrevendo meu livrinho sobre Computer Underground, talvez coloque disponivel na rede, se nao achar editora. Primeiro, logico, registrar, depois, vou ver o que fazer com o dito. To tentando tambem fazer a web page do BE e o chato e' que to com vontade de colocar uns scripts em JAVA, ainda por cima. Gosto de escrever, mas programar e' algo legal. Nao consegui ainda fazer encontros regulares em Sampa, mas to travando contatos com gente que, se e' wanna-be, pelo menos nao da' bandeira de ser. Ainda vou escrever como e' que e' o wanna-be ideal, aquele que o veterano pode ate' ajudar a iluminar o caminho. Po^, nao e' super inteligencia que distingue um verdadeiro fucador de micro. Bom, nao vou soltar a lebre antes da hora.

Ai' vao alguns arquivos que fiz, sempre dentro da otica de contar o milagre, mas nao o Santo. Ja' falei sobre desconfianca, agora e' sobre esconderijos e outros truques. Advirto que e' pura retorica. So' sei que se eu sou capaz de imaginar esses lances que coloco no Barata Eletrica, tem gente que ja' deve ter feito. Nao tenho mais dezoito anos. Alguem em algum lugar, tem muito mais tempo e disposicao para pensar nisso ha' bem mais tempo do que eu. Tive contato com gente do qual pude absorver muito, por osmose. Da' para "cheirar" coisas no ar. O negocio e' saber somar 2 + 2. Ninguem realmente ensina o caminho das pedras. Muitas vezes, so' fala que isso existe. O resto e' "Se segura malandro, que sorrindo se chega mais facil ate' o meio do inferno". Entendeu? Nao? E' um troco que vi num filme

do Hugo Carvana. Mas acho que tem tudo a ver.

HACKERS: O FILME E A VIDA REAL

Que que posso escrever sobre esse filme? Primeiro lugar, o inicio: Um bando de policiais, numa verdadeira operacao de guerra, todo mundo de arma na mao, com coletes a prova de bala, metralhadoras, faltando so' a trilha sonora da SWAT ("tcham, tcham, etc"). O objetivo? Invadir uma casa de familia (classe media?) americana. E', imagina voce terminar de tomar seu cafe' e a sua casa parecendo um bunker sendo invadido. Assim comeca o filme. Corta para o tribunal: "Eu sentencio o reu a ficar longe de qualquer computador ou telefone tonal ate' os dezoito anos de idade". Close para um garotinho de 13 anos, cabelos pretos, penteado JFK, vestindo terninho olhar para os pes, aquele jeitinho de birra, tipo: "po!-e-o-meu-brinquedo" chorar no banco dos reus, que cobre 90% do corpo dele.
Anos depois, na vespera dos dezoito, la' esta' ele (o ator Jonny Lee Miller) invadindo o computador de uma estacao de TV para tirar do ar o discurso de um politico racista e substituir por um filme qualquer.

E', eu gostei do filme.

Pior de tudo, nao fui o unico. Mais ruim ainda, so' ficou uma semana em cartaz aqui em Sao Paulo e foi por acidente que fiquei sabendo. Paciencia. Talvez porque reclamei demais do "The Net", as distribuidoras nao quiseram fazer propaganda. Vou saber..

O fato e' que e' o filme mais realista feito sobre hackers que andou pintando na ultima temporada. "Os que nao sabem nada sobre hacking vao adorar a trama e os que manjam do assunto vao adorar a mensagem" - Emmanuel Goldstein, (ver www.mgmua.com/hackers). Bem que ta' na moda colocar um personagem assim nos filmes. O ultimo filme de James Bond tinha um, parecia alguem que conheco. Mas foi o primeiro filme que conta como e' mais ou menos a vida, no tal chamado "Computer Underground". Tem ate' hacker wanna-be no filme. Nao to falando que todos os caras que conheco sao como aqueles personagens, sao estereotipos que estao na tela. Mas da' pra sentir que houve uma pesquisa, uma curiosidade em mostrar algo mais que feitos de meninos-progidio do mundo atual. Ate' a etica hacker aparece no filme, junto com trechos do Hacker Manifesto, assim como a Engenharia Social. Fica dificil apontar o que os caras esqueceram de colocar. Ah, sim. Existe fantasia e coisas completamente fora da real, do mesmo tipo que apontei sobre o "The Net". Mas botando tudo numa balanca, e' so' um filme, pombas. Com direito a final feliz.

Continuando, apos essa invasao da estacao de TV e' que a historia se desenvolve. O garotinho, agora com 18, se muda para cidade grande e.. vai para o College. Se apaixona no mesmo instante em que preenche sua ficha de matricula. Eh, fucadores tambem amam. A menina (Angelina Jolie), aquele tipo de garota meio androgina de rosto, mas labios carnudos e o corpo no lugar, passa um trote nele, que e' calouro e portanto merece tudo o que um "bixo" tem tem direito. O cara toma um banho, vestido. Tudo bem. Ele nao leva muito a serio. Reprograma o sistema de incendio do lugar para dia D, hora H, minuto M, segundo X comecar a inundar todas as salas e corredores do predio. E fica de guarda-chuva, esperando a passagem da procissao.

Como ta' afim da garota, tambem aproveita para alterar sua matricula. Vai para a mesma sala em que a veterana e' monitora. Claro que a essa altura do filme, ja' tem colega dele que ja' sacou que o cara e' diferente, ja' convidam o dito para os locais onde a acao rola e acao vira mais uma especie de "momento educativo" onde se fala alguns lugares comuns do mundo de rato de computador, como a questao de senhas faceis vs dificeis, os livros que servem de fonte de informacao (tipo o Jargao, livros coloridos, etc). Esqueci de comentar que ninguem sabe que o dito e' o famoso Zero Cool, responsavel por um virus que fez isso e aquilo (uma referencia a

internet worm de Morris, um estudante de 19 anos que "fechou" a rede com o seu virus).

So' para finalizar, na discoteca onde esse pessoal se reune, pintam mais dois cliches do mundo de fucador (que tem varios cliches, of course). Um e' o wanna-be que quer provar que merece entrar no grupo, mesmo sem saber muito (dentro do grupo ira' aprender mais). So' que, da mesma forma que no mundo real, ninguem tem paciencia de bancar o mestre pro guri e este decide fazer algo audacioso para chamar a atencao. Entrar num computador super dificil de uma empresa petrolifera. Tudo bem. Consegue. So' que como e' burro, nao se previne o bastante, e' pego e o dark-side-hacker da empresa, que tinha o seu proprio "esquema malevolo" de sacanagem por debaixo do pano no mesmo computador, que faz ele? Ah, tem uma invasao no sistema? A chamada veio desse telefone aqui, na rua tal? Ta' bom. Avisa o Servico Secreto (pra prender o coitado) e manda um memo p. diretoria avisando que o moleque foi responsavel pelo desaparecimento de X milhoes de dolares com o trabalho dele.

Que e' quase um outro cliche da vida real, quando gente de dentro da empresa faz uso da invasao para ocultar um trabalho feito internamente. Ou dito de outra forma: "vamos usar um virus colocado pelo guri como desculpa para aquele balanco que nao deu certo". Aqui no Brasil o buraco e' mais embaixo para esse tipo de coisa, por conta dos "caixa-dois", mas pode acontecer em qualquer lugar, sem duvida.

"Hackers - Piratas Informaticos" causa um pouco de estranhamento, a primeira vista. Afinal de contas, coloca um mulher como fucadora de micro. E isso e' muito raro. Nao sei porque, mas em Londres, onde fui ver o congresso AAA (Access All Areas) haviam umas tres ou quatro, numa multidao de talvez trezentos. E em Berlim, no Caos Computer Club, havia apenas uma, na reuniao especifica onde fui. Por um acaso, duas das poucas mulheres que conheci em Londres no tal congresso tinham um fisico atraente e uma ate' tinha semelhanca fisica com a atriz do filme (uma das razoes pelas quais ate' hoje to xingando o fato de nao ter ido ao CCC de Bielefeld, Alemanha - tinha ate' carona e motivo mais serio, mas o tempo e grana eram muito curtos). Mas isso e' uma ou duas (ou tres ou quatro) no meio de centenas. Donde pode-se dizer que o filme ta' meio por dentro, ainda. A competicao que ocorre depois e' viagem na maionese, no entanto. Do meu ponto de vista.

Mas quanto aos sonhos do cara, nota dez. Um fucador de micro na maior parte do tempo so' curte o computador e os amigos com quem troca informacoes.

Esquece completamente como e' que sao seres normais. Quando se chega na fase do "16-horas-na-frente-do-micro-to-ligado", a ideia de ter que ir num lugar para encontrar alguem, conhecer, depois checar se tudo bem, esperar o talvez, insistir, quebrar a cara, insistir, quebrar a cara, ate' que pinta (talvez) alguma coisa, e' loucura. Nao tem futuro. O sonho do Dade (Zero Cool) no filme e' tipico. Uma mulher, deusa, que chega no cara, puxa pelo colarinho e fala: "To^ falando com voce, porra! Vamos logo pro carro que depois das seis tem fila no motel que eu gosto". Essa imagem mental e' bastante forte. Lembro que foi mais ou menos assim, quando completei meu primeiro ano como Net-cidadao. O Centro de Computacao da USP fechou o laboratorio um final de semana, ai', como eu nao tinha modem (alias ate' hoje nao tenho) fui sair na cidade, ver uma outra forma de passar o tempo.

O filme tem centenas de porens, alguns interessantes, como o lance de ter personagem real que foi colocado na tela, como o Emmanuel Goldstein (vulgo Eric Corley), editor da 2600 - Hacker Quaterly. Que por sinal, gostou do filme. Tem tudo para se tornar um cult. Quando o vilao se esconde atras de uma identidade falsa, escolhe o nome de Babage (um dos primeiros a imaginar o computador). O computador onde o wanna-be tenta entrar e' um Gibson, sobrenome de um famoso autor de livros e contos "cyber". Um cara comentou que "Cyberspace" nao aparece no filme inteiro, sinal que a briga dos hackers contra a rotulacao "cyberpunk" deu algum resultado (ja' que

punk, para alguns americanos seria denominacao de cara que serve de mulher na cadeia, coisa que no vocabulario ingles britanico - para quem nao sabe os vocabularios dos EUA e da Inglaterra nao batem - denomina estilo de contra-cultura anarquista). Claro que aquela quantidade de graficos de video de clip que e' colocada em algumas cenas, para caracterizar o uso de computador nao tem nada a ver. Por outro lado, a quantidade enorme de tempo que um fucador de micro gasta para fazer um acesso e' algo que quase passa batido. So' no inicio e esporadicamente no filme, se fala do tempo que se gasta para fazer coisas mais simples. Linguagem cinematografica?

Por outro lado, nao existe sequencia mais emocionante do que o mapa da cidade que, via modificacao grafica, fica cada vez mais parecido com uma placa de circuitos de um computador. E' arrepiante. Principalmente porque e' uma forma nova de encarar a realidade. Quando voce pensa que e' o lugar onde voce saca seu dinheiro e' um terminal de acesso via protocolo X.25, que tem outra rede de computadores encarregada dos sinais de trafego, computadores fazendo suas ligacoes telefonicas, computadores fazendo a previsao do tempo, etc, etc tudo isso e' o ambiente onde o ser humano, pelo menos o ser urbano, vive. Controlado pelo computador.

A fucacao retratada no filme e' quase que exclusivamente aquela que chama a atencao da Midia. A dos garotos rebeldes que querem alterar ilegalmente o sistema operacional de alguns computadores. Nada a ver com o fato de que isso e' apenas uma pequena fracao do computer underground. Tem muito mais gente envolvida com varias partes especificas, como pirataria de programas, clonagem ilegal de telefones celulares (coisas que nao sao estimuladas no filme, ainda bem), e aspectos mais profundos como o design de novos computadores. A parte do uso dessa tecnologia como forma de integrar o homem com o seu semelhante e o aprendizado que ela estimula e' mencionado muito de passagem. Nenhum grande fucador se considera um prodigio, apesar do ego inflado que alguns tem. Apenas se veem como caras com alguma inteligencia que se deram ao trabalho de devorar literatura que incluiu manuais de quatrocentas ou quinhentas paginas. Mas .. nao e' o fim o mundo de dificil, tambem, e'? Tudo depende de quao fissurado em micro a pessoa e'. Basta ir fucando, que se chega la'.

UNIX - MELHOR QUE WINDOWS 95?

Historia:

No inicio, era o verbo ... Tinha um carinha, chamado Ken Thompson, que trabalhava nos laboratorios da Ma Bell (ou Bell Laboratories, como queira). Um lugar de pesquisa, responsavel por varias inovacoes, tecnologia nova, etc...o elemento tinha um programa chamado Space Travel, que executava os movimentos dos planetas do sistema solar e para executar o dito, usava um mainframe da General Electric. Pagando pelo uso, que era uma forma comum de se usar computador, tanto naquela epoca como no dia de hoje. Da mesma forma que hoje se usa um modem p. conectar a internet e se paga uma BBS pra isso, naquele tempo se usava um modem e um terminal especifico para poder se programar alguma coisa.

Bom, qualquer um que use BBS ligada a rede internet descobre rapidamente que uma hora por dia nao e' muita coisa. E nao e' facil "debugar" erro por erro de um programa. O Space Travel precisava de muito tempo de computador para funcionar. A alternativa era um minicomputador, chamado PDP-7. So' que o sistema operacional do dito era algo nao muito legal (fedia, dito de uma outra forma). Em vez de se contentar com isso, Thompson desenvolveu o Unix para rodar no PDP-7. Ai' pode "rodar" o Space Travel.

Ai', legal, problema resolvido. Mas a mocada da Bell curtiu o lance. E Thompson desenvolveu uma linguagem nova, chamada B. Como a primeira versao do UNIX tinha sido feita em assembly, usou tal linguagem como base p. a

segunda versao. Ai', um outro colega de trabalho, o Dennis Ritchie refinou a coisa e transformou essa linguagem B na C e e' por isso que hoje quase todo o sistema tem o codigo fonte em C.

Po, fantastico. Um sistema operacional decente para rodar num computador relativamente barato, para a epoca. So' que a Bell, que era subsidiaria da AT&T, nao podia vender o dito. Mandaram as fontes entao para universidades e centros de pesquisa, a precos irrisorios. E isso nao so' divulgou a coisa, como introduziu varios aconchambramentos feitos por milhares de estudantes que acabaram sendo incorporados ao codigo, como o editor VI e o EMACS.

A propria Microsoft licenciou o Unix e produziu o XENIX, mas estava ocupada com o MSDOS e a coisa ficou para a Santa Cruz Operation, so' para se ter uma ideia como o dito e' bom. O que o DOS foi para o mercado de micros mono-usuario, o UNIX e' para o mercado multi-usuario. Ate' hoje. So' para se ter uma ideia, tem varios clones do mesmo, tais como o Edix (Edisa), Sox (Cobra), Digix (Digirede), Renix (Villares), Sor (Prologica). O Sox foi totalmente desenvolvido no Brasil.

Descricao:

Basicamente, e' um sistema operacional complexo, multi-usuario (cada um pode alegremente pensar que e' unico, a nao ser nas horas em que o sistema fica lotado e o computador fica mais lento), multi-tarefa (pode-se compilar um programa, acessar a internet via ftp, gopher, lynx, etc ao mesmo tempo, etc), mais de 200 comandos e programas.

Uma parte do sistema faz a interface com o hardware, gerencia a memoria, a entrada/saida: o Kernel, que nada mais e' que um programa em C compilado que e' mantido na memoria, desde que acontece o boot (vale lembrar que um sistema multi-usuario de pequeno e medio porte e' mantido funcionando 24 horas por dia, na maioria das vezes so' da' o boot da maquina uma vez por dia, quando e' bem gerenciado). Outra parte e' o "shell", que faz a interface entre o usuario e a maquina. O DOS tambem tem sua shell e o ambiente Windows nada mais e' que um tipo de shell, so' para dar um exemplo. A ultima parte sao os programas e ferramentas que o sistema operacional tem para executar suas tarefas.

Na verdade o DOS imitou varias ferramentas do Unix, mas como o usuario padrao nao se da' ao trabalho de aprender, acaba indo para coisas tipo Mane-DOS. Isso, so' para dar uma ideia para os nao iniciados.

Consideracoes:

Quando se comeca a entender o labirinto deste sistema operacional, o entendimento de uma linguagem como o C e' quase intuitivo. Alias, a linguagem de programacao Shell, que para a mocada seria o equivalente a programacao em arquivos .BAT e' quase C. Pode-se dar no' em pingo d'agua e construir bancos de dados, fazer calculos, sistemas de gerenciamento de arquivo, com base em muitos poucos comandos, sem precisar de compilador.

Existe o modo grafico, chamado X-Windows que e' uma especie de interface com mouse. Tecnicamente semelhante ao Windows. Existe um grupo de fucadores na Internet, pelo mundo afora, desenvolvendo o que se chama de "Emulador de Ambiente Windows" para Unix, se nao me engano. Para poder rodar jogos e programas "interessantes" neste ambiente. Funciona, embora seja uma coisa feita sem interesse comercial, quer dizer, e' uma mocada que se voluntariou sem nenhuma perspectiva de ganhar grana com isso. Ultima vez que li a respeito, varios programas ja' podiam ser rodados em Unix, embora em um ou outro programa, acessar caracteristicas como o help poderia fazer a sessao cair (o Ctrl-Alt-Del seguido de Enter no Windows 3.1).

Falando nisso, existe alguns clones que merecem referencia, tais como o Minix, que foi desenvolvido para micros PC. Este e' interessante porque tem disponivel uma versao demo na internet, junto com um FAQ. Tem seus fas e grupos de discussao. A versao Demo permite ter um "gostinho" do que e' sistema operacional, com varios comandos e cabe em disquete 5 1/4 de 360 kbytes. So' que e' comercial. Tem que se pagar uma grana para se usar, nao

existe por ai' nem se encontra facil.

Outro e' o Unix BSD que e' uma versao do Unix para PC fruto do Computer Science Research Group (CSRG) da U.C. Berkeley. E' gratuito, pode-se encontrar um "mirror" do dito no ftp.unicamp.br. Parece que da' um trabalho para configurar para uso como servidor, por exemplo, mas alguns falam que e' bem estavel depois que consegue.

O Linux, esse ja' e' fruto da iniciativa de Linus Torvalds. Centenas de pessoas se voluntariaram para ajudar a fazer o dito funcionar. Nada de pagamento. O troco funciona, e' atualizado regularmente e conta com "espelhos" onde se pode copiar sem remorso de estar pirateando. Usa 40 a 250 megabytes de espaco em disco ou 12 numa versao CD-ROM (so' se instala o necessario pro dito funcionar). Qualquer duvida ou defeito, e' so' mandar cartinha para uma lista na internet e eles (os voluntarios de plantao ou um usuario qualquer que manja) manda a resposta, ou o "remendo" para o problema. Quer mais vantagens? E' sistema de 32 bits e nao se paga nada pelos programas. Ta' tudo disponivel na Internet. Mais ou menos uns 50 disquetes em versao Slackware. Varios servidores Internet estao baseados neste sistema operacional.

Pontos ruins:

E' dificil falar deles, mas fica muito suspeito nao escrever nada. Bom, o Unix e' um sistema operacional pra Macho. Ou machucado, tambem pode ser. Primeiro que, a nao ser que voce se dedique a aprender os comandos, vai pastar. E' arido. Bem arido. Se nao houver um motivo forte, nao aprende. Alias, nao precisa aprender muito. Num PC, a pessoa acaba assumindo a funcao de gerente de sistema, que e' o responsavel pelas tarefas de instalacao de software/atualizacao e apagamento de arquivos inuteis do micro. Agora num sistema de grande porte e medio porte, voce e' responsavel pelo gerenciamento de sua "area" que e' um subdiretorio no qual so' o dono pode colocar programas. Quero dizer com isso e' que o sistema Unix foi feito por fucadores que queriam fucar. E' um submundo do qual poucos sabem. Tanto que existe a figura chamada Super-usuario. E' o unico com "privilegios" para instalar novos usuarios, programas, enfim fazer a manutencao do sistema. Deveria ser um cara extremamente inteligente, capaz e responsavel. Deveria ser. Na verdade, a diferenca de capacidade entre um super-usuario e um fucador de nivel medio e' em muitos casos algo burocratico. O fucador sabe mais, mas nao recebe 13o salario pela ajuda que da'. Uma merda. Quando se tem uma empresa com um sistema Unix multi-usuario funcionando, os Super-usuarios que manjam do riscado sao verdadeiras "vacas sagradas". Botar um sistema Unix no PC em casa e' um ato de coragem, vontade de aprender ou puro masoquismo. As vezes as tres coisas junto. Prinicipalmente numa sociedade como a brasileira, onde a pirataria de software e' quase a norma, nao importa o que diz a legislacao. A questao da seguranca no Unix tambem e' o mesmo que discutir sexo dos anjos.

Tambem nao e' facil se encontrar software comercial portado para esse ambiente. A pessoa tem que depender de material disponivel na rede ou criar o que precisa. O que acaba acontecendo mais e' uma convivencia dos dois sistemas.

Pontos Bons:

Ja' coloquei um monte. Mas curto Unix principalmente por saber que daqui a dez anos o que aprendi ainda sera' valido. Existe um monte de codigo ja' pronto e disponivel para consulta, otimos manuais on-line, depositos de informacoes sobre duvidas. No caso do Linux, nao e' preciso se preocupar com pirataria. Outra coisa e' que a Internet e' altamente compativel com o Unix. Tem sempre alguem que pode te ajudar com alguma dica ou coisa que se pode fazer (eu pelo menos encontro, aqui na USP e na Internet). Nao existe

preocupacao com virus de computador, tambem. Cavalos de troia podem ate' existir, mas sao raros. E pode-se facilmente portar o codigo fonte de um programa para funcionar em outro. Ninguem te enche o saco se voce usa o codigo fonte disponivel na rede e implementa ou melhora funcoes, pelo contrario, aplaudem e pedem pra voce mandar uma copia do "remendo".

Para concluir:

E' uma aventura. Sou um cara muito suspeito p. falar desse sistema operacional. Todo mundo que consegue fazer alguma coisa com ele acaba se apaixonando. Se voce quiser ter algum gostinho pela coisa, procure o subdiretorio "pub/simtelnet/msdos/textutil" de qualquer "mirror" da Simtel e faca download dos arquivos do PICNIX que e' uma implementacao do dito cujo em DOS. Outra coisa e' que algumas implementacoes de Shell do Unix, tem um monte no Simtel20. Qualquer duvida, faca download do arquivo 00INDEX.ALL ou 00INDEX.ZIP (melhor) e procure. O demo do MINIX tambem e' uma boa. Para finalizar, se voce pretende conversar com hackers estrangeiros, e' bom aprender um basico.

COMO ESCONDER SEUS DADOS, VALORES E SEGREDOS

Para comecar, nao e' um assunto no qual me sinto a vontade para falar. Primeiro, porque nao acredito na ideia de esconderijo "perfeito", nem de segredo. Tudo depende de se encontrar a chave certa para a fechadura. Apesar do titulo, vou comecar com o lance de segredo.

Quando se tem um segredo, so' se tem uma forma de guarda-lo: nao partilha-lo com ninguem. Esquecer que existe. Ser indiferente ate' a existencia do dito, a nivel interno. E quando mais importante, mais dificil, fica a coisa. Precisa uma certa disciplina ou cara de pau. Experimenta por exemplo conversar com uma menina (nota: para tornar o artigo de compreensao mais facil, prefiro usar elementos de nivel bem geral). Vamos acrescentar o lance de que e' alguem interessante, do ponto de vista fisico (ex:fica bem de biquini fio-dental). Tenta fingir que nao quer nada com ela e comeca um papo "desinteressado". Para qualquer um que esta' do lado de fora, e' idiota pensar que vai ter sucesso. As mulheres usam fio-dental por varias razoes, uma delas porque sabem que isso faz o cara arregalar os olhos durante um papo "informal". A voz da pessoa fica alterada. E' dificil fingir a indiferenca. A fala nao e' a unica forma de uma pessoa se expressar. Embora hajam excecoes, tudo o que a pessoa transmite para outra e' transmitido em duplicata, pelo corpo. So' para se ter uma ideia, voltando a voz, pode-se fazer um analisador de registro vocal, q. registra a tensao na fala, fato que pode ou nao revelar uma mentira. E nao e' coisa de Servico Secreto, apareceu ja' em revista de eletronica. E claro que uma mulher tem seus truques pra avaliar seu interesse por ela, coisas que nao tem nada ver com a pergunta "voce esta' afim de mim". O unico jeito de esconder o interesse pela menina seria nao conversar nem com ela, nem com ninguem, a respeito dela.

A tensao gerada existencia de um segredo, e' stress e o corpo libera esse stress de varias formas. Se uma pessoa acabou de fazer algo que o pensamento abomina ou quer manter secreto, a tensao acumulada e' tamanha que faz a pessoa assumir um comportamento que evidencia culpa. Isso, obvio, em se tratando de pessoas inexperientes. Mas mesmo pessoas experientes sabem que nao ha' antidoto para "ser pego em flagrante". No maximo, consegue-se manter silencio total. Se o assunto e' trazido a baila, ha' tensao e alguns conseguem enrolar ate' mudar o objetivo da conversa. E' algo complicado. A propria mudanca de assunto pode ser sintoma de algo "errado". Ouvi falar que quando uma pessoa e' entrevistada p. emprego, em alguns lugares, fazem-se perguntas, do tipo o que a pessoa come de manha.

Como se trata de um assunto inofensivo, a pessoa responde sem mentir e isso cria um parametro pro entrevistador saber quando a resposta e' verdadeira. Quanto mais relaxada a pessoa conseguir ficar, melhor consegue esconder um segredo. Quanto mais falar, mais cai em contradicoes, a longo prazo. Sobre como esconder valores: tudo depende do que esta' sendo escondido, suas dimensoes e quem esta' procurando. Quando viajava de carona na Europa, conversei com gente que fazia isso direto, seis meses por ano. Me contaram a historia de um sujeito que cansou de encontrar gente teve seus pertences roubados. Como? O cara usava a mochila como travesseiro e dormia com o passaporte, carteira, etc, na ponta do sleeping bag, perto dos pes. Ai', ia o bandido usava uma gilete e cortava a extremidade do saco. Roubava os valores. Muitos faziam essa besteira, tinha virado moda esconder desse jeito, os gatunos ja' sabiam. E normalmente sabem, porque prestam mais atencao a esses detalhes. Se voce quiser aprender sobre a arte de esconder coisas, leia um livro, do tipo "Papillon" ou "Expresso da Meia-Noite". Se o lance e' procurar coisas, leia "a carta roubada" de Edgar Allan Poe. Mas leia o livro. O filme nao da' esse tipo de detalhe. Se os habitos de quem procura sao conhecidos, pode-se esconder melhor. E' mais facil "achar" coisas escondidas do que achar bons lugares para esconder as coisas.

Por exemplo: voce pode considerar o stereo do carro como devidamente escondido no porta-malas, mas nao se seu objetivo e' contrabandear o dito. Porque o ladrao comum nao vai abrir o porta-malas de tudo quanto e' carro ja' que nao existe, que seja do meu conhecimento, habito generalizado de esconder coisas no porta-malas. Mas a Policia Fedral pode e deve abrir seu porta-malas, se tiver qualquer duvida. Contrabando e' crime, eles podem receber um elogio a mais da chefia, por cumprirem com a obrigacao.

Donde a grande conclusao: A partir do momento em que existe um habito de se esconder isso aqui ou ali, o lugar ja' deixou de ser secreto. Ha' tambem o fato da pessoa ter "flagrado" voce colocando seu som naquele lugar. Um truque muito bom de filme (da minha infancia) era o lance da vela oca. So' que hoje, ninguem usa vela. Livro oco, tem uma descricao no livro "Sem perdao" do Frederick Forsyth, onde, num conto, e' ilustrado o processo de se fazer isso. Tudo bem, desde que seja algo pequeno. O grande lance e' quando o objetivo e' esconder isso de alguem que se interessa pelo assunto do livro. Quase ninguem se interessa por Biblia, por exemplo. Mas se a unica leitura do sujeito for best-sellers, fica estranho aquela leitura na estante. Mesmo que nao interesse, chama a atencao.

Uma estrategia e' a do redirecionamento. Explicando de forma simples: va' num supermercado. A nao ser que o gerente esteja doido para se livrar de uma mercadoria, os produtos com o preco mais caro sao aqueles quase ao nivel dos olhos. A pessoa tem que se agachar para descobrir os produtos mais baratos. Como a maioria das pessoas tem varios graus de preguica ou mesmo nao gostam de ficar agachando, isso funciona razoavelmente bem. Entao, aproveitando, e' so' esconder em lugares onde a pessoa nao tem o costume de olhar. Uma historia do tempo da lei seca, nos EUA, e' a de um barco que a guarda-costeira investigou por conta de uma denuncia. Procuraram de popa a proa, mas nao encontraram nada. Ate' que o comandante resolveu beber um copo d'agua. Tava la' a bebida. Na caixa d'agua. E' provavel que os traficantes de drogas tenham um monte de historias semelhantes para contar.

O que me lembra a questao da revista corporal. Em caso de assalto, isso e' comum. Usar bolsinhas de viagem "especiais" que ficam por dentro ja' me ajudaram a preservar os valores em muita viagem por ai'. Colocar dinheiro dentro da meia tambem pode ser uma boa. Apesar que em alguns tipos de assalto, o meliante resolve deixar a vitima pelada com uma unica folha de talao de cheque para pegar o taxi, so' pro cara aprender a deixar uma grana pro assaltante. Roubo de tenis importado e' comum. Deixar na virilha, tipo dentro da cueca, pode funcionar, mas incomoda e pode cair. Dentro da calcinha (para as mulheres) acho dificil, ja' que as de hoje sao quase do

tamanho da etiqueta. No sutia, pode funcionar. Quando o assaltante ta' dopado e nao quer tirar uma lasquinha da mulher. Ha' alternativas mais drasticas, como no livro "Papillon" de Henri Charriere. Os caras tinham um tipo especial de objeto, vagamente parecido com um vibrador nas duas pontas, que servia para o sujeito guardar dinheiro e etc.. O problema e' que todo dia o dito, no banheiro, o cara tinha que tirar (obvio) e colocar de novo. Diz no livro que uma vez foi barra, segurar durante alguns dias a vontade de satisfazer as necessidades. Ja' li na Playboy que um cara tentou contrabandear alucinogeno engolindo camisinhas cheias dele, junto com iogurte. Uma estourou durante a viagem. Ele sobreviveu a experiencia.

Outro teve que operar para tirar um pacote de coca que ficou grudado no estomago. Ja' li tambem que houve o caso de uma mulher que contrabandeava droga dentro de um cadaver empalhado de um bebe. Um agente da Policia Federal estranhou que o dito ficou seis horas quieto, sem chorar. Uma que costuma acontecer na fronteira americana e' o uso de mulheres com implantes cheios de coca. Como americana tem mania de ir no cirurgiao para aumentar o seio, quando nao os tem ja' "naturalmente" grandes, algumas enchem o dito de coca ou outra droga, antes de cruzar a fronteira do Mexico com os EUA. E se "fodem" porque existe um equipamento chamado fluoroscopio (nao lembro mais onde li isso), que sabe distinguir coca de silicone. Normalmente, o pessoal da guarda fronteirica sabe como procurar.

Seguranca dos dados, isso ja' e' uma especializacao. Basta dizer que isso de sistema seguro, perfeitamente seguro, nao existe. Pode-se esconder os dados do pessoal com quem voce trabalha, do seu chefe, mas de gente que tem mais experiencia de computacao que voce, muito dificil. Porque tem um fator, o de acesso. Aqueles dados que voce nunca acessa, e' facil criptografar usando PGP ou outro software com opcao de criptografia, como o PKZIP 2.04g (tem um outro cujo nome esqueci). O problema todo e' quantas vezes os dados vao ser acessados. Se forem acessados em ambiente de rede, varias vezes por dia, e' preciso inventar uma solucao e pior, treinar os funcionarios no uso dela. Se voce for o unico usuario, disciplinar-se para sempre esconder seus dados. E isso nao e' facil.

Mesmo que consiga, o melhor e' nao confiar em opcoes de criptografia de programas americanos, alem dos citados acima. A criptografia e' regulamentada como municao perante a legislacao americana, significando que nada realmente bom e' liberado para venda a nivel mundial. Mas vamos a algumas dicas simples.

O maior problema da seguranca de qualquer tipo de dado e' garantir que a pessoa que vai lidar com o micro sabe o suficiente para nao fazer besteira, mesmo gente com experiencia detona a winchester de vez em quando, ou deixa entrar um virus de computador. Ou seja, um fator de inseguranca que sempre existe. Para evitar isso, normalmente so' outra pessoa, tipo o tecnico, realmente sabe o que tem dentro. A nivel bem basico, basta salvar o material em disquete e guardar num cofre. Se nao existe ninguem que saiba muita coisa sobre micro no lugar onde voce trabalha, basta renomear o arquivo para algum nome criptico, tipo "CATZO.DAT" ou "TTZZ.SYS". Se quiser garantir mais um pouco, altere o atributo para "hidden". Usando a estrategia do redirecionamento, pode colocar ele no subdiretorio DOS ou WINDOWS. Claro que nao funciona com subdiretorios inteiros ou grande numeros de arquivos. Alem disso, isso e' algo muito pobre. O subdiretorio inteiro pode ser apagado para a instalacao de novo software, por exemplo, e ja' existe software para apagar arquivos que estejam sobrando.

Para subdiretorios, uma possibilidade que existia, no DOS, ainda existe, era uma ferramenta simples, que pintou na PC Magazine, atualmente disponivel em qualquer sitio mirror da Simtel. Nao lembro o nome, so' o que fazia. Mexia na tabela de alocacao de arquivos, FAT. O subdiretorio ficava invisivel exceto para ferramentas como PCTOOLS e outros softwares do genero. O problema foi quando comecei a escrever uns trabalhos num subdiretorio escondido e tempos depois formatei o disquete sem salvar esse

material. Tava tao secreto que esqueci dele. Alias nao tenho certeza se formatei ou quando formatei, so' sei que nunca mais encontrei o dito. Para quem quiser experimentar alguma coisa semelhante, aperta a tecla ALT e ao mesmo tempo as teclas 2, 5 e 5. Dessa forma aparece um caractere "invisivel" na tela. Da' pra fazer n variacoes e truques com isso. So' que tambem e' algo pobre. Outra e' fazer um subdiretorio com letras minusculas. O DOS transforma letras minusculas em maiusculas no prompt. Sem um programa que mexa com a FAT, fica dificil entrar no subdiretorio.

Para cada coisa que voce esconda, alem do fator humano, existe outro, que e' mais serio. E' a questao do acesso a informacao que se quer proteger. Quanto maior a necessidade de acesso mais atrapalhado fica o uso de sistemas de seguranca. Um exemplo sao os funcionarios que simplesmente escrevem a senha num papel perto do terminal, para nao esquecer. E quando o processo de alcancar a informacao fica automatizada, a precaucao com a seguranca fica esquecida. Por exemplo, os arquivos que forem criptografados precisam ter seus originais apagados. E nao se apaga nada com o comando DEL do DOS. O espaco do arquivo fica livre, mas os bits que compoem a informacao ficam la', e podem ser des-apagados com um comando undelete ou com o Norton Utilities ou o DEBUG. O PC Farias e o Peter North, do caso Iran-Contras, descobriram isso, da forma mais dificil. No Linux ou no Unix, isso nao existe. E' quase impossivel recuperar um arquivo. Uma forma de garantir esse apagamento e' o uso de programas que "obliteram" o espaco do disco com "lixo". Tem varios. Inclusive uma ferramenta de rato de computador , que desenvolveram nos EUA, que detona com o disco rigido inteiro da pessoa, no caso de invasao pelo Servico Secreto.

Um lance que esta' pintando na Internet e' usar arquivos de imagens para esconder dados. Isso existe no Macintosh. Infelizmente, nao sei muito sobre esse tipo de computador. No lance de esconder dados na Internet, isso pinta muito com warez. Sao subdiretorios escondidos em maquinas abertas para download de arquivo via FTP. O sistema e' semelhante ao do alt + numero, e funciona. So' que, quem faz isso, muda o nome do subdiretorio de semana em semana e se pintar sinal de que muita gente ta' acessando, todo o software pirata que fica(ria) naquele subdiretorio escondido vai para outro site, e so' quem e' do ramo fica sabendo. Como nao manjo muito de pirataria, nao posso dar maiores informacoes sobre isso.

BBSES QUE NAO ESTAO NO MAPA

BBS UNDERGROUND

No Brasil, nao existem muitas. Nem sao para existir em grande quantidade. Sao as BBSes e sistemas de computacao sintonizados exclusivamente para gente que sabe o que quer e nao e' so' aprender. Nada de escutar suplicas de gente que nao pergunta: "meu, como e' que usa Blue Beep ou faz um Break-in"? Nada disso. So' algumas pessoas acessam porque so' algumas pessoas sabem da existencia e ate' para se saber da existencia e' preciso conhecer alguem ou ser indicado por alguem que ja' faca parte da coisa. Ou ter conhecimento tecnico para achar as ditas.
sao as BBSes "subterraneas".

Lenda? Nao. A pessoa as vezes tem material, sabe que os amigos querem ter acesso a esse material. A turminha nao tem tempo de se encontrar e tambem nao querem que qualquer wanna-be ou reporter venha tomar o tempo e linha telefonica. Por outro lado, as vezes nem sempre a coisa e' feita legalmente. As vezes, e' um setor de uma BBS ou sistema computacional que esta' sub-utilizado (quer dizer: o Sysop ou Super-Usuario do computador nao sabe que tem uma BBS instalada nele). O dia em que o dono descobre, o site e' mudado para outro lugar. Afinal de contas, o conceito de BBS comeca com um lugar onde alguem liga para ler arquivos que contenham mensagens. E' tao simples fazer um arquivo escondido em algum lugar de um computador cheio..

As pessoas no caso tem que usar obrigatoriamente nomes-codigo ou apelidos, (como o brasileiro chama) e frases-senhas para evitar enganos. Talvez arquivos criptografados por uma senha de uso comum.

Isso, a um nivel mais basico. Qualquer fucador de micro pode pensar ou ja' pensou ou mesmo ja' fez um esquema do genero. O DOS permite a qualquer um com um pouco de conhecimento, fazer gato e sapato de qualquer disco rigido. Provavelmente o Windows95 deve facilitar ainda mais as coisas, pois estimula as pessoas a nao olharem o que tem na winchester. Para nao falar mal so' da Microsoft, a verdade e' que quanto mais complicado o sistema operacional, maior o numero de "becos" onde e' possivel esconder qualquer coisa. O OS-2 deve ter as mesmas facilidades. O Unix e os VAXs da vida tambem tem.

A nivel mais avancado, existem na Internet, computadores cujos sistemas sao adulterados para permitir o armazenamento de arquivos WAREZ e sabe-se la' o que mais. A partir de um determinado numero de dias, de acessos, ou mesmo sem nenhuma razao especial, todo o sistema e' devolvido ao estado original. Todos os conteudos "perigosos" sao deletados. E nao e' tao simples fazer o acesso. Sao necessarios softwares especiais para entrar no(s) lugare(s). Existe por exemplo, versoes de programas de ftp para windows especificas para sites desse genero, que so' sao distribuidas para um publico nao muito grande e validas por pouco tempo, as vezes uma ou duas semanas apos a divulgacao. Nao, nao adianta me perguntar como sei disso ou onde descobri sobre esse ultimo paragrafo. Sao migalhas de informacao de outras pessoas, colhidas pela rede Internet afora. Mas se eu fui capaz de pensar tudo isso, sei que existe.

WAREZ BBS

Gozado, no "meu" tempo, a gente chamava pura e simplesmente de bbs pirata. Mas hoje, o que era pirataria ganhou a denominacao WAREZ. Nao que tenha que se seguir essa denominacao. Mas subentende-se algo diferente. Quando se fala de pirataria, isso inclui a venda de programas sem pagar direitos autorais. A pirataria dita "warez" (tal como me foi explicado e ja' vi defendido em varios lugares por ai') tem mais a ver com experimentar um software p. ter certeza de que supre tudo aquilo que anunciam acerca dele. Dessa forma, para carregar esse nome, tem uma serie de normas que devem ser obedecidas nesses sites ou bbses estocando violacoes de direito autoral. Existem warez especificos para jogos, outros para sistemas operacionais e utilitarios, etc. Em cada um deles, o programa tem que estar corretamente armazenado. Tintin por tintin. E' o mais proximo possivel que se consegue do pacote original. Se o cara vai fazer o upload do pacote, tira primeiro o numero de serie (que iria denuncia-lo) ou registro, depois faz varios arquivos ou mesmo imagens de disco (existe software que permite xerocar o disquete inteiro p. um arquivo em winchester). E um textinho (fora do conjunto de arquivos, p. nao misturar) explicando como "desempacotar" a coisa. Nao tenho certeza se e' assim mesmo, mas um cara, durante um IRC me explicou assim. Nao chequei mesmo. Na internet, existem listas de tais sites, que circulam, tal como descrito no texto acima. O publico e' mais amplo, mas tambem e' so' por indicacao. No http://www.allcomm.com/hackers tem uma reportagem como foi feita uma blitz em cima de uma BBS desse genero.

VIRUS BBS

Aqui no Brasil ja' ouvi falar da Viegas BBS, que era mais sobre como fazer cavalos de troia em Turbo Pascal, Dbase e ate' Lotus 1-2-3. Seria em Minas Gerais, mas nunca tive certeza se era invencao do cara ou realidade. Tempos depois, a figura negou ter falado no assunto. Recentemente, outra pessoa me passou o arquivo geral de index (para o pessoal da internet seria o ls-lR ou 00INDEX.ALL) da dita. O numero do telefone vinha junto, cifrado. Mas ...

um carinha para quem emprestei o dito me disse que era totalmente ocupado, quase todas as horas do dia. So' mesmo um hacker ou phreaker, para conseguir acessar a dita. Para se associar, seria necessario fazer o download do tal arquivo e fornecer algo que a BBS nao teria em estoque. Ou, caso de uma pessoa que conheci, descobrir uma forma de quebrar a seguranca da BBS e avisar o administrador (sim, porque se o administrador descobrir a falha sozinho, ele conserta e volta-se a estaca zero).

Mas tem um pouco mais de historia. A primeira a nivel internacional, foi a de Sofia, na Bulgaria. Em numeros anteriores do Barata Eletrica, esta historia ja' foi contada. Uns tempos atras eu tinha o numero DDI para la'. Tava cogitando conseguir alguem para me ajudar a acessar a dita quando fui para a Argentina e descobri que o cara ja' tinha trocado de telefone. Alem do que, telefonar para o antigo bloco comunista e' algo do outro mundo.(Tipo fazer DDD para qualquer lugar no nordeste as 16:40 de qualquer dia da semana, aqui em Sao Paulo). Mas, voltando a dita cuja, o estudante que montou a coisa, Todor Todorov numa reportagem para o periodico Virus News International - maio 93) coisa nao deu muito certo, pelas mesmas razoes (la' dentro tambem e' ruim para fazer DDD). Vai saber o que e' lenda e o que e' verdade.

Lenda ou nao, nos EUA a coisa vingou, em parte por causa do excelente sistema telefonico e paixao pelo lado "marginal" da coisa. Afinal, foi la' que surgiram os primeiros computadores e inclusive o conceito de virus, a partir de uma teoria de Von Neuman. Para descrever em poucas palavras, uma Virus BBS nao difere muito de qualquer bbs. Apenas o conteudo dos arquivos e' perigoso. Mesmo assim, todos os arquivos sao corretamente classificados em subdiretorios. Programas de virus ficam em subdiretorios nomeados virus. Cavalos de troia em subdiretorios com o nome e cada arquivo de index tem o que o nome do programa/virus. Codigo fonte de virus fica em outro lugar e etc, etc. Existe tambem um subdiretorio para anti-virus e uma sessao de mensagens para comentar as ultimas novidades, assim como sessoes dedicadas a revista (eletronicas) sobre o genero, tipo NUKE, 40HEX, VLAD, CRYPT, MINOTAURO, etc (tem outras, mas esqueci). Ao contrario de algumas bbses, onde nao se sabe se o programa que voce pega esta' ou nao contaminado, nessas BBSes, isso nao existe. Como?

Bom, o fato da pessoa acessar a BBS e' metade da historia. No caso de uma BBS argentina famosa, primeiro a pessoa tem que provar ser capaz de entender assembler o bastante para montar ela propria um virus, ter um projeto de virus razoavelmente bom ou fazer o upload de um. Tendo feito isso, pode ter acesso ao codigo fonte e informacoes sobre todos os outros virus que a BBS tem em seu estoque. Nao adianta tentar enganar o Sysop: ele sabe das coisas, porque ele proprio ja' fez virus de computador. No caso da BBS argentina (tem uma lista que ja' publiquei num numero anterior do Barata Eletrica), nao adianta ameacar nem xingar o cara. Teria que entrar numa fila. Ameacar chamar a policia? Na Argentina (e tambem no Brasil) a legislacao ainda nao chegou nesse ponto. Usando codinomes, a privacidade e' respeitada. Nos EUA, a coisa nao e' assim tao rigida. Em alguns lugares, colecoes de virus e codigos-fonte apenas completam o conteudo, que pode tambem ter dicas de como assustar seu colega de ape, pseudo-manuais de terrorismo e destruicao ou dicas de quebramento de senhas e contravencoes, do tipo que usa cartoes de credito.

Sobre esses ultimos, basta dizer que conhecimento nao e' crime. Na verdade, a maioria dos arquivos e' informacao ultrapassada, mas o pessoal que acessa curte ler e guardar, com o mesmo entusiasmo de um fa de armas de fogo. Pena que o Servico Secreto de la' nao pensa assim. Volta e meia, essas BBSes sao bastante vigiadas e entrar em algumas delas usando seu telefone e endereco verdadeiros e' a mesma coisa que entrar numa lista X, que e' um verdadeiro saco de gatos. Muita paranoia...

==========

(parte 1)

------- Title: Stalking the wily hacker. (includes related articles on the definition of hackers, Intruder versus Tracker, legal constraints and ethics, and computer security resources) Journal: Communications of the ACM May 1988 v31 n5 p484(14) * Full Text COPYRIGHT Assn. for Computing Machinery, Inc. 1988. Author: Stoll, Clifford. Summary: The experience of the Lawrence Berkeley Laboratory in tracking an intruder suggests that any operating system is insecure when obvious security rules are ignored. How a site should respond to an intrusion, whether it is possible to trace an intruder trying to evade detection, what can be learned from tracking an intruder, what methods the intruder used, and the responsiveness of the law-enforcement community are also discussed.

------- STALKING THE WILY HACKER In August 1986 a persistent computer intruder attacked the Lawrence Berkeley Laboratory (LBL). Instead of trying to keep the intruder out, we took the novel approach of allowing him access while we printed out his activites and traced him to his source. This trace back was harder than we expected, requiring nearly a year of work and the cooperation of many organizations. This article tells the story of the break-ins and the trace, and sums up what we learned. We approached the problem as a short, scientific exercise in discovery, intending to determine who was breaking into our system and document the exploited weaknesses. It became apparent, however, that rather than innocuously playing around, the intruder was using our computer as a hub to reach many others. His main interest was in computers operated by the military and by defense contractors. Targets and keywords suggested that he was attempting espionage by remotely entering sensitive computers and stealing data; at least he exhibited an unusual interest in a few, specifically military topics.

Although most attacked computers were at military and defense contractor sites, some were at universities and research organizations. Over the next 10 months, we watched this individual attack about 450 computers and successfully enter more than 30. LBL is a research institute with few military contracts and no classified research (unlike our sister laboratory, Lawrence Livermore National Laboratory, which has several classified projects). Our computing environment is typical of a university: widely distributed, heterogeneous, and fairly open. Despite this lack of classified computing, LBL's management decided to take the intrusion seriously and devoted considerable resources to it, in hopes of gaining understanding and a solution. The intruder conjured up no new methods for breaking operating systems; rather he repeatedly applied techniques documented elsewhere. whenever possible, he used known security holes and subtle bugs in different operating systems, including UNIX, VMS, VM-TSO, EMBOS, and SAIL-WAITS. Yet it is a mistake to assume that one operating system is more secure than another: Most of these break-ins were possible because the intruder exploited common blunders by vendors, users, and system managers.

Throughout these intrusions we kept our study a closely held secret. We deliberately remained open to attacks, despite knowing the intruder held system-manager privileges on our computers. Except for alerting management at threatened installations, we communicated with only a few trusted sites, knowing this intruder often read network messages and even accessed computers at several computer security companies. We remained in close touch with law-enforcement officials, who maintained a parallel investigation. as this article goes to press, the U.S. FBI and its German equivalent, the Bundeskriminalamt (BKA), continue their investigations. Certain details are therefore necessarily omitted from this article. Recently, a spate of publicity surrounded computer break-ins around the

world [23, 33, 37]. With a few notable exceptions (e.g., [24, 36]), most were incompletely reported anecdotes [7] or were little more than rumors. For lack of substantive documentation, system designers and mangers have not addressed important problems in securing computers. Some effrts to lighten security on common systems may even be misdirected. We hope that lessons learned from our research will help in the design and management of more secure systems. How should a site respond to an attack? Is it possible to trace the connections of someone trying to evade detection? What can be learned by following such an intruder? Which security holes were taken advantage of? How responsive was the law-enforcement community? This article addresses these issues, and avoids such questions as whether there is anything intrinsically wrong with browsing through other people's files or with attempting to enter someone else's computer, or why someone would wish to read military databases. Nonetheless, the author holds strong opinions on these subjects.

DETECTION

We firt suspented a break-in when one of LBL's computers reported an accounting error. A new account had been created without a corresponding billing address. Our locally developed accounting program could not balance its books, since someone had incorrectly added the account. Soon afterwards, a message from the National Computer Security Center arrived, reporting that someone from our laboratory had attempted to break into one of their computers through a MILNET connection. We removed the errant account, but the problem remained. We detected someone acting as a system manager, attempting to modify accounting records. Realizing that there was an intruder in the system, we installed line printers and recorders on all incoming ports, and printed out the traffic. Within a few days, the intruder showed up again. We captured all of his keystrokes on a printer and saw how he used a subtle bug in the Gnu-Emacs text editor [40] to obtain system-manager privileges. At first we suspected that the culprit was a student prankster at the nearly University of California. We decided to catch him in the act, if possible. Accordingly, whenever the intruder was present, we began tracing the line, printing out all of his activity in real time.

ORGANIZING OUR EFFORTS

Early on, we began keeping a detailed logbook, summarizing the intruder's traffic, the traces, our suspicions, and interactions with law-enforcement people. Like a laboratory notebook, our logbook reflected both confusion and progress, but eventually pointed the way to the solution. Months later, when we reviewed old logbook notes, buried clues to the intruder's origin rose to the surface. Having decided to keep our efforts invisible to the intruder, we needed to hide our rcords and eliminate our electronic messages about his activity. Although we did not know the source of our problems, we trusted our own staff and wished to inform whoever needed to know. We held meetings to reduce rumors, since our work would be lost if word leaked out. Knwing the sensitivity of this matter, our staff kept it out of digital networks, bulletin boards, and, especially, electronic mail. Since the intruder searched our electronic mail, we exchanged messages about security by telephone. Several false electronic-mail messages made the intruder feel more secure when he illicitly read them.

MONITORS, ALARMS, AND TRAFFIC ANALYSIS

We needed alarms to instantly notify us when the intruder entered our system. At first, not knowing from which port our system was being hit, we

set printers on all lines leading to the attacked computer. After finding that the intruder entered via X.25 ports, we recorded bidirectional traffic through that set of lines. These printouts proved essential to our understanding of events; we had records of his every keystroke, giving his targets, keywords, chosen passwords, and methodologies. The recording wa complete in that virtually all of these session were captured, either by printer or on the floppy disk of a nearby computer. These monitors also uncovered several other attempted intrusions, unrelated to those of the individual we were following.

Off-line monitors have several advantages over monitors embedded in an operating system. They are invisible even to an intruder with system privileges. Moreover, they gave printouts of the intruder's activities on our local area network (LAN), letting us see his attempts to enter other closely linked computers. A monitor that records keystrokes within an operating systm consumes computing resources and may slow down other processes. In addition, such an monitor must use highly privileged software and may introduce new security holes into the system. Besides taking up resources, on-line monitors would have warned the intruder that he was being tracked. Since printers and personal computers are ubiquitous, and because RS-232 serial lines can easily be sent to multiple receivers, we used this type of off-line monitor and avoided tampering with our operating systems. The alarms themselves were crude, yet effective in protecting our system as well as others under attack. We knew of researchers developing expert systems that watch fror abnormal activity [4, 35], but we found our methods simpler, cheaper, and perhaps more reliable. Backing up these alarms, a computer loosely coupled into our LAN periodically looked at every process. Since we knew from the printouts which accounts had been compromised, we only had to watch for the use of these stolen accounts. We chose to place alarms on the incoming lines, where serial line analyzers and personal computers watched all traffic for the use of stolen account names. If triggered, a sequence of events culminated in a modem calling the operator's pocket pager. The operator watched the intruder on the monitors. If the intruder began to delete files or damage a system, he could be immediately disconnected, or the command could be disabled. When he appeared to be entering sensitive computers or} downloading sensitive files, line noise, which appeared to be network glitches, could be inserted into the communications link. In general, we contacted the system managers of the attacked computers, though in some cases the FBI or military authorities made the contact.

Occasionally, they cooperated by leaving their systems open. More often, they immediately disabled the intruder or denied him access. From the intruder's viewpoint, almost everyone except LBL detected his activity. In reality, almost nobody except LBL detected him. Throughout this time, the printouts showed his interests, techniques, successes, and failures. Initially, we were interested in how the intruder obtained system-manager privileges. Within a few weeks, we noticed him exploring our network connections--using ARPANET and MILNET quite handily, but frequently needing help with lesser known networks. Later, the monitors showed him leapfrogging through our computers, connecting to several military bases in the United States and abroad. Eventually, we observed him attacking many sites over Internet, guessing passwords and accounts names. By studying the printouts, we developed an understanding of what the intruder was looking for. We also compared activity on different dates in order to watch him learn a new system, and inferred sites he entered through pathways we could not monitor. We observed the intruder's familiarity with various operating systems and became familiar with his programming style. Buried in this chatter were clues to the intruder's location and persona, but we needed to temper inferences based on traffic analysis. Only a complete trace back would identify the culprit. TRACE

BACKS Tracing the activity was challenging because the intruder crossed many networks, seldom connected for more than a few minutes at a time, and might be active at any time. We needed fast trace backs on several systems, so we automated much of the process.

Within seconds of a connection, our alarms notified system managers and network control centers automatically, using pocket pagers dialed by a local modem [42]. Simultaneously, technicians started tracing the networks. Since the intruder's traffic arrived from an X.25 port, it could have come from anywhere in the world. We initially traced it to a nearby dial-up Tymnet port, in Oakland, California. With a court order and the telephone company's cooperation, we then traced the dial-up calls to a dial-out modem belonging to a defense contractor in McLean, Virginia. In essence, their LAN allowed any user to dialout from their modem pool and even provided a last-number-redial capability for those who did not know access codes for remote systems.

Analyzing the defense contractor's long-distance telephone records allowed us to determine the extend of these activities. By cross-correlating them with audit trails at other sites, we determined additional dates, times, and targets. A histogram of the times when the intruder was active showed most activity occurring at around noon, Pacific time. These records also demonstrated the attacks had started many months before detection at LBL. Curiously, the defense contractor's telephone bills listed hundreds of short telephone calls all around the United States. The intruder had collected lists of modem telephone numbers and then called them over these modems. Once connected, he attempted to log in using common account names and passwords. These attempts were usually directed at military bases; several had detected intruders coming in over telephone lines, but had not bothered to trace them. When we alerted the defense contractor officials of their problem, they tightened access to their outbound modems and these were no more short connections. After losinig access to the defense contractor's modems, the still undeterred intruder connected to us over different links. Through the outstanding efforts of Tymnet, the full X.25 calling addresses were obtained within seconds of an attack. These addresses pointed to sources in Germany: universities in Bremen and Karlsruhe, and a public dial-up modem in another German city. When the intruder attacked the university in Bremen, he acquired system-manager privileges, disabled accounting, and used their X.25 links to connect around the world. Upon recognizing this problem, the university traced the connections to the other German city. This, in turn, spurred more tracing efforts, coordinating LBL, Tymnet, the university, and the German Bundespost. Most connections were purposely convoluted. Figure 1 summarizes the main pathways that were traced, but the intruder used other connections as well. The rich connectivity and redundant circuits demonstrate the intruder's attempts to cover his tracks, or at least his search for new networks to exploit. Besides physical network traces, there were several other indications of a foreign origin. When the intruder transferred files, we timed round-trip packet acknowledgments over the network links.

Later, we measured the empirical delay times to a variety of different sites and estimated average network delay times as a function of distance. This measurement pointed to an overseas origin. In addition, the intruder knew his way around UNIX, using AT&T rather than Berkeley UNIX commands. When stealing accounts, he sometimes used German passwords.

In retrospect, all were clues to his origin, yet each was baffling given our mind-set that "it must be some student from the Berkeley campus.""

A STINGER TO COMPLETE THE TRACE

The intruder's brief connections prevented telephone technicians from determining his location more precisely than to a particular German city. To narrow the search to an individual telephone, the technicians needed a relatively long connection. We baited the intruder by creating several files of fictitious text in an obscure LBL computer. These files appeared to be memos about how computers were to support research for the Strategic Defense Initiative (SDI). All the information was invented and steepest in governmental jargon. The files also contained a mailing list and several form letters talking about "additional documents available by mail" from a nonexistent LBL secretary. We protected these bogus files so that no one except the owner and system manager could read them, and set alarms so that we would know who read them. While scavenging our files one day, the intruder detected these bogus files and then spent more than an hour reading them.

During that time the telephone technicians completed the trace. We celebrated with milk shakes made with homegrown Berkeley strawberries, but the celebration proved premature. A few months later, a letter arrived from someone in the United States, addressed to the nonexistent secretary. The writer asked to be added to the fictitious SDI mailing list. As it requested certain "classified information," the letter alone suggested espionage. Moreover, realizing that the information had traveled from someone in Germany to a contact in the United States, we concluded we were witnessing attempted espionage. Other than cheap novels, we have no experience in this arena and so left this part of the investigation to the FBI.

BREAK-IN METHODS AND EXPLOITED WEAKNESSES

Printouts of the intruder's activity showed that he used our computers as a way station; although he could become system manager here, he usually used LBL as a path to connect to the ARPANET/MILNET. In addition, we watched him used several other networks, including the Magnetic Fusion Energy network, the High Energy Physics network, and several LANs at invaded sites. While connected to MILNET, this intruder attempted to enter about 450 computers, trying to log in using common account names like root, guest, system, or field. He also tried default and common passwords, and often found valid account names by querying each system for currently logged-in accounts, using who or finger. Although this type of attack is the most primitive, it was dismayingly successful: In about 5 percent of the machines attempted, default account names and passwords permitted access, sometimes giving system-manager privileges as well. When he succeeded in logging into a system, he used standard methods to leverage his privileges to become system manager. Taking advantage of well-publicized problems in several operating systems, he was often able to obtain root or system-manager privileges. In any case, he searched file structures for keywords like "nuclear," "sdi," "kh-11," and "norad." After exhaustively searching for such information, he scanned for plain-text passwords into other systems.

This proved remarkably effect ive: Users often leave passwords in files [2]. Electronic mail describing log-in sequences with account names and passwords is commonly saved at foreign nodes, allowing a file browser to obtain access into a distant system. In this manner he was able to obtain both passwords and access mechanisms into a Cray supercomputer. Typical of the security holes he exploited was a bug in the Gnu-Emacs program. This popular, versatile text editor includes its own mail system, allowing a user to forward a file to another user [40]. As distributed, the program uses the UNIX Set-User-ID-to-Root feature; that is, a section of the program runs with system-manager privileges. This movemail facility allows the user to change file ownership and move files into another's directory. Unfortunately, the program did not prevent

someone from moving a file into the systems area. Aware of this hole, the intruder created a shell script that, when executed at root level, would grant him system privileges. He used the movemail facility to rename his script to masquerade as a utility periodically run by the system. When the script was executed by the system, he gained system-manager privileges. This intruder was impressively presistent and patient. For example, on one obscure gateway computer, he created an account with system privileges that remained untouched until six months later, when he began using it to enter other networked computers. On another occasion, he created several programs that gave him system-manager privileges and hid them in system software libraries. Returning almost a year later, he used the programs to become system manager, even though the original operating-system hole had been patched in the meantime. This intruder cracked encrypted passwords. The UNIX operating system stores passwords in publicly readable, but encrypted form [26]. We observed him downloading encrypted password files from compromised systems into his own computer. Within a week he reconnected to the same computer, logging into new accounts with correct passwords. The passwords he guessed were English words, common names, or place-names. We realized that he was decrypting password filed on his local computer by successively encrypting dictionary words and comparing the results to password file entries. By noting the length of time and the decrypted passwords, we could estimate the size of his dictionary and his computer's speed. The intruder understood what he was doing and thought that he was not damaging anything. This, alas, was not entirely true. Prior to being detected, he entered a computer used in the real-time control of a medical experiment. Had we not caught him in time, a patient might have been severely injured. Throughout this time the intruder tried not to destroy or change user data, although he did destroy several tasks and unknowingly caused the loss of data to a physics experiment. Whenever possible, he disabled accounting and audit trails, so there would be no trace of his presence. He planted Trojan horses to passively capture passwords and occasionally created new accounts to guarantee his access into computers. Apparently he thought detection less likely if he did not create new accounts, for he seemed to prefer stealing existing, unused accounts.
(Continua na proxima edicao - se houver)

PERGUNTAS MAIS FREQUENTES SOBRE "ANONYMOUS REMAILERS"

por:
Andre Bacard, Author of
"Computer Privacy Handbook"
[FAQ Updated October 25, 1995]
[Links at http://www.well.com/user/abacard]
OBS: A traducao foi feita por um colaborador e nao foi revisada

This article offers a nontechnical overview of "anonymous" and "pseudo-anonymous" remailers to help you decide whether to use these computer services to enhance your privacy. I have written this especially for persons with a sense of humor. You may distribute this (unaltered) FAQ for non-commercial purposes.

O que e um remailer?

Remailer e um servico que torna o seu e-mail anonimo. O remailer permite que voce envie correspondencia eletronica para um news group da USENET ou

para uma pessoa sem que esta saiba a procedencia da mensagem, seu NAME ou seu ENDERECO eletronico. Atualmente a maioria do remailer sao gratis.

Por que voce usaria remailer?
Talves voce seja um engenheiro de computador que deseja expressar sua opiniao sobre algum produto, e nao deseja que seu chefe o reconheca pois ele pode nao gostar. Talves voce viva em uma comunidade intolerante com relacao a sua condicao social, opiniao politica e religiosa. Talves voce esteja procurando um novo emprego e queira demonstrar isto para seu chefe atual. Talvez voce queira se promover. Talvez voce seja um dedo-duro com medo de retaliacao. Voce sente que caso critique o seu governo, o Big Brother ira te monitorar. Talvez voce apenas nao queira que as pessoas "flaming" o seu endereco eletronico. Resumindo, existe inumeras razoes para que voce, cidadao honesto, use 1 remailer.

Como o remailer funciona?
Vamos a um exemplo. Um remailer muito popular na internet e mantido por Johan Helsingius, presidente de uma companhia finlandesa que auxilia transacoes economica via internet. Seu endereco "an@anon.penet.fi" aperece frequentemente em new's group controversos. Suponhamos que voce leia uma mensagem de uma mulher maltratada pedindo ajuda. Voce
pode responde-la no mesmo endereco . O computador ira
apagar o seu verdadeiro nome e endereco eletronico (o cabecario do seu e-mail), substituindo-o por um outro endereco qualquer e envia sua mensagem para a mulher maltratada. O remaler ira notificar o seu endereco anonimo (ex. an345.anon.penet.fi). Voce pode usar este servico gratuitamente para enviar uma mensagem anonima para quem quer que seja, ate mesmo para pessoas que nao utilizam o servico. O computador envia detalhadas instrucoes sobre o sistema.

Existem muitos remailer?
Atualmente existem algumas duzias de remailers publicos que qualquer um pode usar gratuitamente (existem alguns remailers especializados que permitem seus usuarios enviarem mensagem para apenas alguns Usenet groups. Este tipo nao sera discutido aqui). Remalers costumam surgir e desaparecer continuamente. Primeiro, eles precisam de equipamento e pessoal para funcionar e segundo eles nao produzem nenhum remuneramento.

Por que os remailers sao gratuitos?
Existe uma resposta simples. Como os administradores do remailer podem cobrar pessoas que querem o maximo de privacidade? Eles nao podem pedir o numero do cartao de credito ou um cheque. No futuro, remailer poderao se tornar um servico pago. Privacidade e valiosa.

Por que pessoas mantem remailer se nao recebem dinheiro para isso?
Pessoas montam remailer para o seu uso pessoal, nao se importando em compartilha-lo conosco. Joshua Quittner, co-autor do high-tech thriller "Mother's Day", entrevistou o Sr. Helsigius para revista Wired. Helsigius disse:

> "E importante expressar certas opinioes sem que todo mundo saiba quem e voce. Um dos melhores exemplos foi o debate a respeito de CALLER ID nos telefones. As pessoas estavam realmente aborrecidas pois a quem estava do outro lado da linha sabia perfeitamente quem estava falando. Em coisa como o telefone, se da muita importancia em ser anonimo, e seria desagravel que se tirasse isso das pessoas. Eu penso a mesma coisa dos E-mails."

"Vivendo na Finlandia, eu vi bem de perto como as coisas estavam na extinta URSS . Se voce eventualmente tivesse uma fotocopiadora ou mesmo uma maquina de escrever la, voce teria de registrar-la e eles iriam pegar exemplo de como a sua maquina escreve, para poder identificar uma carta. Eu acho isso um absurdo. E algo como registrar todos as suas possiveis maneira de se comunicar para o estado, como ter que assinar tudo na Rede. Nos temos que sempre poder identificar voce."

Qual a diferenca entre anonimo e pseudo-anonimo remailers?
A maioria das pessoas usam a expresao "anonymous remailer" para os dois tipo de remailers. Isto pode gerar alguma confusao. Um "PSEUDO-anonymous" remailer e basicamente uma conta que voce compartilha com o operador do remailer. Anon.penet.fi (descrito acima) e um PSEUDO-anonymous remailer. Isto significa que Juft, o operador e seus assistentes sabem o seu endereco eletronico (e-mail address) real. A sua privicaidade depende do poder e integridade de Juft para proteger seus arquivos. Pense em num PSEUDO-anonymous remailer como quase anonimo remailer. Oque isto significa? Forcado de alguma maneira o operador do remailer pode revelar sua verdadeira identidade. Na Finlandia a policia obrigou Juft a revelar pelo menos uma identidade verdadeira. A facilidade do PSEUDO-anonymous remailer e que eles sao faceis de usar. Se voce pode enviar um e-mail voce pode compreender um PSEUDO-anonymous remailer. O preco que voce paga pela facilidade na utilizacao e a menor seguranca que ele proporciona. O realmente remailers anonimos sao completamente diferentes. The good news... Eles sao muito mais seguros do que os PSEUDO-anonymous. The bad news...
Eles sao muito mais dificeis de utilizar.
Existem basicamente dois tipos de remailers anonimos. Eles sao "Cypherpunk remailer" e Lance Cottrell's "MixMaster remailer". Eu mencionei remailers no plural caso voce queira realmente privacidade voce deve mandar suas mensagens atraves de dois ou mais remailers. Se for bem feito voce pode estar seguro que ninguem (nenhum operador ou snoop (oque i isto) podera ler seu nome e mensagem juntos. Isto significa anonimato verdadeiro. Na pratica ninguem pode forcar o operador do remailer a fornecer sua identidade, simplesmente porque o operador nao tem nenhuma pista de quem e voce. Cypherpunp e MixMaster e familia sao demasiado tecnicos para serem descritos nesta pequena FAQ. Voce pode obter links para detalhes tecnicos checando: Anonymous Remailer FAQ no endereco-http://www.well.com/user.abacard

Oque significa remailer ideal?
Um remailer ideal e (a) facil de usar. (b) Rode em um sistema que realmente faz oque diz. E deve esta bem protegido dos intrusos.

Como deve agir um usuario responsavel de remailer?
Um usuario responsavel: (a) envia mensagens de tamanho razoavel. Arquivos binarios demoram muito para serem transmitidos. Transmita apenas arquivos importantes. Remailers nao foram desenvolvidos para transmitir mensagens de piramides e correntes da felicidade, por exemplo.

Quem e um usuario responsavel?
Segue texto de um administrador de remailer.
"Este remailer foi usado indevidamente no passado, a maioria dos usuario se escondia atras do anonimato para assediar outra pessoas na rede. Eu pretendo criar impecilios para estes usuarios. Vamaos manter a rede um lugar amigo e produtivo. Usar um remailer para assediar alguem e um ato totalmente abominavel. Eu revelarei o verdadeiro enderesso do usuario que proceder desta maneira para a policia. Verdadeiro remailer nao toleram assedio ou atividade crominal, comunique este tipo de atividade ao

administrador do remailer."

Os remailer sao realmente confiaveis (apenas para paranoicos)

Para a maioria das tarefas de pouca seguranca resposta pessoal a uma carta os PSEUDO-anonymous remailers com senha de seguranca sao indiscutivelmente mais seguros doque e-mail normal. Entretanto ate mesmo melhor do planos humanos tem fraquesas. Suponhamos, por exemplo, que voce e um funcionario publico que descobre que seu chefe esta sendo subornado. E seguro usar PSEUDO-anonymous remailers para enviar evidencia do crime para o orgao governamental responsavel? Alguns pontos devem ser bem examinados.
(a) o operador do remailer pode interceptar suas mensagens indo e voltando do remailer. Ista da ao operador prova de que voce esta delatando seu chefe corrupto. Isto pode colocalo em perigo.
(b) talvez o remailer seja uma armadilha governamental destinada a detectar atividade criminal na rede. O operador pode ser o parceiro corrupto do seu chefe.
(c) Hackers podem fazer magica com computadores. E possivel que Hackers civis ou do governo penetrem no remailer (sem que o operador perceba) e ler sua mensagem.
(d) E possivel que o Big Brother monitore e armazene todas as mensagens, incluindo senhas, entrando e saindo do remailer.
Por estas razoes, documentos altamente secretos (alta privacidade) nao devem ser mandados por PSEUDO-anoymous remailer. Deve-se usar Cypherpunk ou MixMaster enviando as mensagens atraves de mais de um remailer anonimo. Desta maneira somente o primeiro sabe o seu verdadeiro endereco mas nao tem como saber o destino final da correspondencia. Alem disso as mensagem podem ser criptografadas (PGP).

Informacao tecnica e software.

Pode-se obter informacao tecnica, incluindo software visitando Anonymous Remailer FAQ no Web Site: http://www.well.com/user/abacard

Remailer Technical Info and Software

> You can link up to technical remailer material, including the software, by visiting the Anonymous Remailer FAQ at my Web site [address below].

Andre, have you written other privacy-related FAQs?

> I'm circulating an (1) Anonymous Remailer FAQ, (2) E-Mail Privacy FAQ, (3) (Non-Technical) PGP FAQ for Novices, and (4) ALPHA.C2.ORG Remailer FAQ. To get these FAQs,
>
> Visit my WEB site: http://www.well.com/user/abacard
>
> Or send me this e-mail: To: abacard@well.com
> Subject: Help
> Message: [Ignored]

DIARIO DE UM USUARIO AOL

OBS: Este mail veio da lista de piadas que assino. O autor ou a pessoa que traduziu teve seu nome editado, por razoes ja' explicadas acima.

Este mail eh dedicado ao Toto (o caozinho de Miami), que eh da AOL! ;-)
Alias, acho que foi ele que escreveu esse diario... :-DDDDDDD
(brincadeira, heim Toto... :-))

Muitos ja devem ter lido este diario no meu site, mas aqui estah ele de novo para os que nao leram e para os novos assinantes da lista:

-+-+-

18/julho - tentei me conectar com a america online. eu ouvi que que este eh o melhor servico on-line que se pode ter. ate' inclui um disco gratis! acho melhor nao gastar esse no caso deles nao me mandarem mais outro! nao consigo conectar. nao sei o que ha' de errado...

19/julho - um cara do centro de suporte tecnico disse que meu computador precisa de um modem. nao vejo porque. ele deve estar tentando me enganar. que tipo de idiota ele pensa que eu sou?

22/julho - eu comprei o modem. nao consigo imaginar aonde isso vai. ele nco encaixa no monitor ou na impressora. estou confuso.

23/julho - eu finalmente tive meu modem instalado. aquele meu vizinho de 9 anos de idade fez isso pra mim. mas o modem ainda nco funciona. eu nao consigo estar on-line!

25/julho - meu vizinho de 9 anos me conectou aa america online. ele eh tao esperto! eu disse ao garoto que ele era um prodigio. mas ele disse que era apenas outro servico. que garoto modesto. ele eh tao esperto e faz esses servicos para as pessoas. de qualquer maneira, ele eh mais esperto que aqueles estupidos que me venderam o modem. eles nem me disseram sobre o tal software de comunicacao. aposto que eles nem sabiam. e por que eles puseram duas entradas para o cabo telefonico atras do modem quando se precisa somente de uma? e porque eles tem um escrito phone quando nao se supoe ligar ele na tomada da parede? eu achei o som da discagem muito divertido! meu, modems sao ensurdecedores! mas o garoto avaliou ele pelo som.

26/julho - o que eh essa internet? eu pensei que eu estava na america online. nao nessa coisa de internet. estou confuso.

27/julho - o garoto de nove anos me mostrou como usar essa america online. eu lhe disse que ele devia ser um genio. ele disse que eh se comparado a mim. talvez ele nao seja tao modesto, apesar de tudo.

28/julho - eu tentei usar o chat, hoje. tentei conversar com meu computador mas nada aconteceu. talvez eu precise comprar um microfone.

29/julho - eu achei esta coisa chamada usenet. eu sai' fora dela porque eu estou conectado aa america online, e nao usenet.

30/julho - essas pessoas dessa coisa de usenet vivem usando letras maiusculas. como eles fazem isso? eu nunca imaginei como se faz para digitar letras maiusculas. talvez eles tenham um outro tipo de teclado.

31/JULHO - EU LIGUEI PARA O FABRICANTE DO COMPUTADOR QUE EU COMPREI PARA RECLAMAR SOBRE NAO HAVER TECLAS PARA LETRAS MAIUSCULAS EM MEU TECLADO. O CARA DO SUPORTE TECNICO DISSE QUE ERA ESSA TECLA CAPS LOCK. POR QUE ELES

NAO ESCREVEM CORRETAMENTE O QUE ISSO FAZ? EU DISSE A ELE QUE EU TINHA UM TECLADO FAJUTO E QUE QUERIA UM MELHOR. E QUE UMA DE MINHAS TECLAS SHIFT NAO E' DO MESMO TAMANHO DA OUTRA. ELE DISSE QUE ERA PADRAO. EU DISSE A ELE QUE EU NCO QUERIA UM TECLADO PADRAO, MAS OUTRO DE QUALIDADE. EU DEVO TER TIDO UMA RECLAMACAO IMPORTANTE PORQUE EU OUVI ELE DIZER PARA O OUTRO CARA DO SUPORTE PARA VIR ESCUTAR NOSSA CONVERSA.

1/AGOSTO - EU ENCONTREI ESTA COISA CHAMADA O ORACULO USENET. ELA DIZ QUE PODE RESPONDER TODAS AS PERGUNTAS QUE EU FIZER. EU ENVIEI 44 PERGUNTAS SEPARADAS SOBRE A INTERNET. EU ESPERO QUE ISSO RESPONDA LOGO.

2/AGOSTO - EU ENCONTREI UM GRUPO CHAMADO REC.HUMOR. EU DECIDI ENVIAR ESTA PIADA SOBRE A GALINHA QUE CRUSOU A ESTRADA. PARA CHEGAR AO OUTRO LADO! HA!HA! EU NCO TINHA CERTEZA SE TINHA ENVIADO DIREITO, ENTCO ENVIEI MAIS 56 VEZES.

3/AGOSTO - EU TENHO OUVIDO SOBRE A WORLD WIDE WEB (LARGA TEIA MUNDIAL). EU NAO SABIA QUE ARANHAS CRESCIAM TANTO ASSIM.

4/AGOSTO - O ORACULO RESPONDEU AS MINHAS PERGUNTAS HOJE. PO, ELE FOI TCO RUDE. EU FIQUEI TAO BRAVO QUE ENVIEI UM MENSAGEM BRAVA SOBRE ISSO AO GRUPO REC.HUMOR.ORACLE. EU NCO TINHA CERTEZA SE TINHA ENVIADO DIREITO, ENTCO ENVIEI MAIS 22 VEZES.

5/AGOSTO - ALGUEM ME DISSE QUE LER O FAQ. PO, ELES NCO PRECISAVAM USAR PROFANIDADE!

6/AGOSTO - ALGUIM MAIS ME DISSE PARA PARAR DE GRITAR EM TODAS AS MINHAS MENSAGENS. QUE ESTUPIDO IDIOTA! NAO ESTOU GRITANDO! NEM SEQUER ESTOU FALANDO! APENAS TECLANDO! COMO ALGUEM PODE DEIXAR ESSES RUDES IDIOTAS IREM PARA A INTERNET?

7/Agosto - Para que ter uma tecla caps lock se supoe-se nao usa-la? Isto eh provavelmente uma coisa extra para custar mais dinheiro.

8/Agosto - Eu li a uma mensagem chamada faca dinheiro facil. Estou tao excitado! Farei montes de dinheiro. Eu segui suas instrucoes e enviei elas a todos os newsgroups que eu pude encontrar.

9/Agosto - Eu fiz meu arquivo de assinatura. Ele tem apenas 6 paginas. Terei de trabalhar nisso algum tempo mais.

10/Agosto - Eu olhei um grupo chamado alt.aol.sucks. Eu li algumas mensagens e eu realmente acredito que a AOL deve ser varrida da face da terra. Estou curioso para saber o que i uma AOL.

11/Agosto - Eu andei perguntando onde encontrar alguma informacao sobre alguma coisa. Um cara me disse para checar o ftp.netcom.com. Tenho procurado mas nao consigo encontrar esse grupo.

12/Agosto - Eu enviei uma mensagem para cada grupo usenet na internet perguntando onde o grupo ftp.netcom.com fica. Tenho esperangas que alguem me ajude. Nco posso perguntar ao goroto, meu vizinho. seus pais disseram que quando ele volta da minha casa ele ri tanto que nao consegue comer, dormir ou fazer sua licao de casa. Entco eles nao querem mais deixar ele vir aqui. Eu tenho um grande senso de humor. Eu nao sei porque o grupo rec.humor nao gostou da minha piada sobre a galinha. Talvez eles apenas so' gostem de piadas obscenas. Algumas pessoas me enviaram respostas sobre minhas 56 mensagens da piada e eles usaram palavroes.

13/Agosto - Eu enviei outra mensagem para cada grupo usenet da internet perguntando onde o grupo ftp.netcom.com esta. Ontem eu tinha esquecido de incluir meu novo arquivo de assinatura que tem apenas 8 paginas. Eu sei que qualquer um ira' querer ler meu poema favorito que eu inclui nele. Eu tambim estou pensando em incluir aquela pequena histsria que eu gosto.

14/Agosto - Algum cara suspendeu meu acesso por causa de algo que eu estava fazendo. Eu disse a ele que nco tinha uma conta em seu banco. Que cara mais surdo!

:-D

MURPHOLOGIA AVANCADA
==========

LEI DE MURPHY:

Se alguma coisa pode dar errado, dara.

COMENTARIO DE FUNARO:

Murphy e um otimista.

COMENTARIO DE BRESSER PEREIRA:

Funaro era um otimista.

COMENTARIO DE NEWTON CARDOSO SOBRE A ORIGEM DA LEI DE MURPHY:

A Lei de Murphy nao foi enunciada por Murphy, mas por outro cara com o mesmo nome.

COROLARIO DE MAILSON:

Dois erros sao apenas um bom comeco.

COROLARIO DE ULISSES A LEI DE MURPHY:

Em qualquer circunstancia, a decisao certa a tomar e determinada pelos acontecimentos posteriores.

LEI SARNEY DE GOVERNO:

Se alguma coisa pode dar errado, dara em triplicata.

LEI JANIO QUADROS:

As coisas so dao certo para depois poderem dar errado.

ADENDO A LEI DE MURPHY:

A equacao "1+1=2" so esta certa se o sinal "=" quiser dizer "muito raramente".

PRINCIPIO INFALIVEL DE MURPHY:

Voce so sabe que uma coisa da errado depois de repetir varias vezes o mesmo erro.

LEI TELE SANTANA:

Nada e tao inevitavel quanto um erro que voce preve.

LEI FREUDIANA:

No momento da erecao ha sempre um marido para atrapalhar.

LEI DO CIENTISTA MALANDRO:

Se sua experiencia fracassou, destrua todas as provas de que tentou.

LEI SODRE DA NACIONALIDADE:

Toda sardinha e portuguesa, mesmo as pescadas no Brasil. Vieram nadando.

AXIOMA MATEMATICO DO IBGE:

UM inflacionado vale mais do que DOIS congelado.

LEI QUERCIA DA PROBABILIDADE:

De dois acontecimentos provaveis, so acontece o menos desejado.

LEI MOREIRA SALES:

Nao ha limite para o ponto a que as coisas ruins podem chegar.

LEI DOROTEA:

Nao ha trabalho tao simples que nao possa ser feito de modo complicado.

OBSERVACAO DE MAE WEST:

Errar e humano, mas a sensacao e divina.

LEI GABEIRA:

A natureza abomina o homem.

LEIS DO FUNCIONARIO MINEIRO:

1 - Nunca seja o primeiro.
2 - Nunca seja o ultimo.
3 - Nunca se ofereca voluntariamente.

PRINCIPIOS DE MARIO GARNERO:

E pouco a pouco que os problemas viram muitos.

PADRAO GLOBO:

Quantidade = 1/Qualidade, ou seja: a qualidade e sempre uma fracao ordinaria.

LEIS DE CAMOES E MOSHE DAYAN:

Toda particula que voa sempre encontra um olho.

LEI DE ENTROPIA DO PMDB:

Se voce derrama uma colher de vinho num tonel de excrementos, nenhum enologo sera capaz de identificar a safra.

LEI ESCADINHA:

Quase tudo e mais facil de enfiar do que de tirar.

LEI DA REGULAMENTACAO DA CONSTITUICAO:

A urgencia varia na proporcao inversa da importancia.

PRINCIPIO ANTONIO CARLOS MAGALHAES:

Quando ele diz que nem morto faria, pregue bem o caixao.

LEI DA CANELADA INEVITAVEL:

Mesmo o objeto mais inanimado tem movimento suficiente para ficar no seu caminho.

Um abraco, turma!

R?????? M???????

OBSERVACAO: Provavelmente esse material foi copiado do livro "Lei de Murphy" (transubstanciacao por Millor Fernandes)

==========
abacard@well.com
Stanford, California
http://www.well.com/user/abacard
Enjoy your privacy...
==========

Bacard wrote "The Computer Privacy Handbook" [Intro by Mitchell Kapor]. Published by Peachpit Press, (800) 283-9444, ISBN # 1-56609-171-3.

==========

CARTAS - DICAS - NOVIDADES -PIADAS

==========

Subject: E dizem que somos perigosos!!

Ola Meu amigo Baratico :-)
  Fico feliz em saber que voce recebeu a sua conta novamente, e quando estara no ar o Barata Eletrica 11??? :-)
  Bom, nao foi so voce que quase ficou sem acesso a rede por culpas de outros, eu mesmo sofri uma pressao enorme dentro da Univ.Fed.Fluminense, sem contar com mais um carinha que perdeu a sua conta dentro da UFRJ pois imprimiu o Barata Eletrica e foi intitulado pessoa nao mais aceita dentro do laboratorio(tsi tsi tsi).

Ha um replay de um e-mail muito curioso para sua analise ;-)
Abracos do amigo B????.....

RESPOSTA: E', meu, nessas horas e' que eu penso: sera' que a censura realmente acabou?

From: M?????? F?????
Subject: Me ajude!!

Caro amigo,
    leio faz tempo sua barata eletronica, te avho bastante inteligente em ralacao a computadores. Te mando esse e-mail esperando uma resposta qualquer que seja ela. Queri que vc me ensinasse macetes e dicas. Espero que no futuro seja parecido com vc.
    um grande abraco...
                        Matheus!!

RESPOSTA:
Gente, acho super-legal receber esse tipo de carta, fico com o ego la' em cima, mas a resposta e' nao. Se eu fosse ensinar dicas, nao seria pelo correio eletronico. Eu escreveria artigos pro Barata Eletrica, que atingiriam um publico maior. Mas isso ta' fora de questao, dar macetes. Enquanto o BE for so' retorica, ainda tem condicoes de sobreviver. Alem disso, tenho um nome a zelar...

NOVIDADES:

From: A????? M?????????? P??????
Subject: O novo dispositivo de Busca

submeta informatica-jb
O NOVO DISPOSITIVO DE BUSCA

Um novo dispositivo de busca chamado Hotbot utiliza "hive computing" (computacao em colmeia) que conecta varias estacoes de trabalho em uma rede de tal modo que cada maquina pode trabalhar em uma parte separada da busca das quase 50 milhoes de paginas existentes agora na World Wide Web. Uma versao beta publica se encontra no endereco:
< http://www.hotbot.com >

New York Times 21 mai 96 C5

From: ????? ?????
To: java-l@di.ufpe.br
Subject: Um furo na seguranca do Java

Oi pessoal,

Peguei essa noticia na parte de infomatica do Brasil OnLine. Eu como todos voces, tambem espero que seja resovido logo.

"Um pesquisador ingljs descobriu um furo na seguranga da linguagem Java que permite que usuarios manipulem alguns objetos e enganem o sistema de seguranga. O pesquisador, David Hopwood, diz em seu site na Web que, explorando um bug no mecanismo que separa as classes JVM (Java Virtual Machine) em diferentes nomes e espagos, um programador pode passar ileso por todas as restrigues de seguranga, incluindo a leitura e escrita de arquivos e a execugco de csdigo nativo no cliente com as mesmas permissues do usuario do navegador.

Segundo Hopwood, o furo ss pode ser consertado atravis do desligamento do Java. O problema afeta todos os navegadores atuais que suportam a linguagem. David ja informou sobre o bug ` JavaSoft, subsidiaria da Sun

Microsystems Inc., de Mountain View, Califsrnia, que desenvolve, distribui e da assistjncia ` linguagem. Segundo o site da JavaSoft na Web, um grupo esta trabalhando no problema e conduz tambim uma revisco geral na seguranga do Java em busca de bugs semelhantes. O site de Hopwood pode ser acessado em http://ferret.lmh.ox.ac.uk/~david/java/bugs/."

Abracos,

D???? C????
e-mail: ????@???????.???.br

Subject: "Dead beef" attack against PGP's key management
Newsgroups: alt.security.pgp,sci.crypt

-----BEGIN PGP SIGNED MESSAGE-----

This post is signed by a forged key for Phil Zimmermann. I forged the key this morning. The key has the same user id and visible key id as an old key for Phil Zimmermann, which he has since revoked.

I should stress that this attack does not in any way weaken the security of PGP's message formats. However, it does expose a problem in the user interface of its key management. Namely, it is fairly easy to forge a key that looks very similar to an existing key. In fact, the only way to distinguish between real and forged keys in general is by the fingerprint and keysize together.

My purpose in posting this is to demonstrate that such forgeries are possible. The lesson is: please do not use the key id alone to identify keys.

Another reason for the public posting of this forgery is to goad the PGP development team into improving the user interface in PGP 3.0, so as to make the detection of such a forgery much easier, if not routine. Derek Atkins has assured me that PGP 3.0 will include a cryptographic hash of the key, for use as a key id. If implemented properly, such a facility would address this attack.

I am not the first to propose this attack. According to Derek Atkins, Paul Leyland first proposed the attack two years ago. Also, Greg Rose successfully mounted a similar attack six months ago, creating a key with user id 0xDEADBEEF, thereby giving rise to the name.

The pseudocode for the attack is as follows:

```
choose random 512 bit prime p
choose random 480 odd x
q = x * ((0xdeadbeef * (p * x) ^ -1) mod 2^32)
do {q += 2^32} while q composite
```

The above bit of pseudocode replaces the original selection of p and q, which are normally just random 512 bit primes. Without having done detailed analysis, I believe that the resulting forged keys are just as good as ordinary PGP keys. Further, the modified key generation is almost as fast as ordinary PGP key generation, and I think I could speed it up a bit more.

The attack took me a few hours to design and code. Any good programmer familiar with PGP could duplicate it easily.

One practical application of this attack is to implement a certain degree of "stealth." Since PGP includes the key id in encrypted messages, it is in most cases possible to identify the recipients of encrypted messages. However, if a lot of people generated keys with the same key id, then it would not be possible to tell from the encrypted message which one was the intended recipient.

Here's the public key I forged, which can be used to check the signature of this message:

```
Key for user ID: Philip R. Zimmermann
1024-bit key, Key ID FF67F70B, created 1992/07/22
Also known as: Philip R. Zimmermann
- -----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAyptNMAAAAEEALRhS3ZCFKLPNF/fZeluh/rNfpgZ5a0ddTBtxJ+1yLIkVurb
HWFFBsrmnA4hU4MhlA8DS/f2gnS0v3zyQ78JOY1SBIJrLdaIPIrh0ZTAZXWoQWDe
Qknm1ZgyLkIRJlt5aDLp+iLJ5sc+LSO5N/DtrL+Htc5MF0AVAWtzPhz/Z/cLAAUR
tCJQaGlsaXAgUi4gWmltbWVybWFubiA8cHJ6QGFjbS5vcmc+iQCVAwUQMWAremtz
Phz/Z/cLAQE//AP/bg9gMOuiBYkFCiyarJ/DIARWDf7e4bWFJloXAyPeBXCITDIw
tuHRJ41yFqnlLmdcuVhXQf/xrH248JyWpHqqED6eOU/PnBHo9IR6H0Fts+O3I+vk
tOYRjuTJy+6JV0s/8VN/Sgh8y6Jm2FGhhzhCp6KHNcTHpUud6iGScaEs/CG0LFBo
aWxpcCBSLiBaaW1tZXJtYW5uIDxwcnpAc2FnZS5jZ2QudWNhci5lZHU+
=Z1mf
- -----END PGP PUBLIC KEY BLOCK-----

Raph Levien

-----BEGIN PGP SIGNATURE-----
Version: 2.6.2

iQCVAwUBMWA2pGtzPhz/Z/cLAQELEQP/fam4tHS8TlMy7SFoUZvC0C4q0ID9Ze5W
rY2D++df4UtAFDITGs4lQqzeq6YCqk51oT8gZAACK6D6UlFgr5roIbgwa74Fxso1
B5mquC9axlOlxZJI1PuK+NflBJqCokuQGtG95ER6vbm4n4RACW43In9SAatIvduN
JfBSLYrAr14=
=V5U6
-----END PGP SIGNATURE-----
```

PARA PREVENIR A TENDINITE...

Me mandaram esse artigo, logo depois de ter escrito sobre a tendinite.

```
Date:         Tue, 17 Aug 1993 15:06:01 +0100
From:         "B.C. Moszkowski"
Subject:      keyboard monitor
```

Below (near the end of this message) is a uuencoded copy of a preliminary version of a very simple keyboard monitor TSR written by me for DOS. It is similar to typewatch. Currently it is fixed at 20 minutes of activity followed by 5 minutes of break. It gives one-minute reminders if the user ignores the break message. I have tried it on a couple of PC's and it seems to work. Any comments welcome. I plan to improve it a bit.

I can put it in the public domain if there is interest. It is given
"as is" and I take no responibility for problems.

Ben Moszkowski

---
begin 600 getup.com
MZ8(!9V5T=7 $ 0$!0;&5A7!I;F<@9'5R:6YG(&)R96%K %EO
M=2!C86X@Y + \
M!W4CCL&Y* "_ "X('#SJXOROP M'"*!#P = DFB05&@\<"Z_%?7@=96,,N
MQ@81 0$N_RX(2Z /A,! 70%+O\N# %5B^Q04U%25U8>!HS+CMO_!A@!@3X8
M 3@$= /IC@ SP*,8 8 ^$ $!=!& /A(! 70_@#X1 0%U..MAD(,^% $ =0>
M/A$! 75C_P84 8,^% $4?%@SP*,4 :(0 :,6 :(1 <8&$@$!NAH!Z#;_ZSV0
M_P86 <8&$@$ Q@81 0"#/A8!!7PGQ@80 0$SP*,4 :,6 ;I8 >@+_^L2D#/
MHQ8!HA$!NCP!Z/K^ZP&0!Q]>7UI96UA=+O\N# &X R [!H =0RX+W([!H(
M=0/K09"X+ ".P+@ 2<)<)<@;&]A9&5D('1O(&UO
M;FET;W(@:V5Y8F]A
Subject: [PIADAS-L] Oragco do pirateador

Programas originais que estais em disco

Copiavel seja vosso conteudo

Venha a nos os seus manuais

Sejam violadas todas as suas protecoes

Assim nessa como nas proximas versoes

As copias nossas de cada dia, nos dai hoje

Perdoai as nossas picaretagens

Assim como nos perdoamos os seus bugs

Nao nos deixei cair na mao da Abes,

e livrai-nos dos virus

BackupBem

M??????? C???????
{Nome apagado pra evitar represalia da ABES - Se a pessoa quiser, entra
no proximo numero}

CORES PRA PAGINAS NA WEB

Ola ???????,

O esquema das cores eh simples: #rrggbb. Os primeiros dois algarismos=20
referem-se a intensidade do vermelho (00 a FF), os outros dois ao verde e=
=20
os dois ultimos ao azul.

Por exemplo:

=09#FFFFFF (todas as cores na sua intensidade maxima) corresponde ao=20
=09=09branco; =20
=09#000000 (ausencia de todas as cores) ao preto;=20
=09#00FF00 a verde;
=09#FF00FF (100% vermelho + 100% azul) a magenta, etc.

Se voce quer uma tabela, abaixo vai uma com 99 cores. Se voce tem acesso=20
ao Corel Draw, pode identificar as cores abaixo pelo nome (fazem parte do=
=20
palette basico do programa).

[<-- Anterior] [Volta para Sum=E1rio]=20
=20

TABELA DE CORES
=20

=20
A tabela abaixo lista a palete b=E1sica de Cores do Corel Draw (99=20
cores) e o c=F3digo hexadecimal #rrggbb correspondente.

[IMAGE]
Black
#000000 [IMAGE]
90% Black
#191919 [IMAGE]
80% Black
#333333 [IMAGE]
70% Black
#4C4C4C [IMAGE]
60% Black
#666666 [IMAGE]
50% Black
#7F7F7F [IMAGE]
40% Black
#999999 [IMAGE]
30% Black
#B2B2B2 [IMAGE]
20% Black
#CCCCCC [IMAGE]
10% Black
#E5E5E5 [IMAGE]
White
#FFFFFF [IMAGE]
Blue
#0000FF [IMAGE]
Cyan
#00FFFF [IMAGE]
Green
#00FF00 [IMAGE]
Yellow
#FFFF00 [IMAGE]
Red
#FF0000 [IMAGE]
Magenta
#FF00FF [IMAGE]
Purple
#9900CC [IMAGE]
Orange

#FF6600 [IMAGE]
Pink
#FF9900 [IMAGE]
Dark Brown
#663333 [IMAGE]
Powder Blue
#CCCCFF [IMAGE]
Pastel Blue
#9999FF [IMAGE]
Baby Blue
#6699FF [IMAGE]
Electric Blue
#6666FF [IMAGE]
Twilight Blue
#6666CC [IMAGE]
Navy Blue
#003399 [IMAGE]
Deep Navy Blue
#000066 [IMAGE]
Desert Blue
#336699 [IMAGE]
Sky Blue
#00CCFF [IMAGE]
Ice Blue
#99FFFF [IMAGE]
Light BlueGreen
#99CCCC [IMAGE]
Ocean Green
#669999 [IMAGE]
Moss Green
#336666 [IMAGE]
Dark Green
#003333 [IMAGE]
Forest Green
#006633 [IMAGE]
Grass Green
#009933 [IMAGE]
Kentucky Green
#339966 [IMAGE]
Light Green
#33CC66 [IMAGE]
Spring Green
#33CC33 [IMAGE]
Turquoise
#66FFCC [IMAGE]
Sea Green
#33CC99 [IMAGE]
Faded Green
#99CC99 [IMAGE]
Ghost Green
#CCFFCC [IMAGE]
Mint Green
#99FF99 [IMAGE]
Army Green
#669966 [IMAGE]
Avocado Green
#669933 [IMAGE]
Martian Green
#99CC33 [IMAGE]
Dull Green

#99CC66 [IMAGE]
Chartreuse
#99FF00 [IMAGE]
Moon Green
#CCFF66 [IMAGE]
Murky Green
#333300 [IMAGE]
Olive Drab
#666633 [IMAGE]
Khaki
#999966 [IMAGE]
Olive
#999933 [IMAGE]
Banana Yellow
#CCCC33 [IMAGE]
Light Yellow
#FFFF66 [IMAGE]
Chalk
#FFFF99 [IMAGE]
Pale Yellow
#FFFFCC [IMAGE]
Brown
#996633 [IMAGE]
Red Brown
#CC6633 [IMAGE]
Gold
#CC9933 [IMAGE]
Autumn Orange
#FF6633 [IMAGE]
Light Orange
#FF9933 [IMAGE]
Peach
#FF9966 [IMAGE]
Deep Yellow
#FFCC00 [IMAGE]
Sand
#FFCC99 [IMAGE]
Walnut
#663300 [IMAGE]
Ruby Red
#990000 [IMAGE]
Brick Red
#CC3300 [IMAGE]
Tropical Pink
#FF6666 [IMAGE]
Soft Pink
#FF9999 [IMAGE]
Faded Pink
#FFCCCC [IMAGE]
Crimson
#993366 [IMAGE]
Regal Red
#CC3366 [IMAGE]
Deep Rose
#CC3399 [IMAGE]
Neon Red
#FF0099 [IMAGE]
Deep Pink
#FF6699 [IMAGE]
Hot Pink

#FF3399 [IMAGE]
Dusty Rose
#CC6600 [IMAGE]
Plum
#660066 [IMAGE]
Deep Violet
#990099 [IMAGE]
Light Violet
#FF99FF [IMAGE]
Violet
#CC66CC [IMAGE]
Dusty Plum
#996699 [IMAGE]
Pale Purple
#CC99CC [IMAGE]
Majestic Purple
#9933CC [IMAGE]
Neon Purple
#CC33FF [IMAGE]
Light Purple
#CC66FF [IMAGE]
Twilight Violet
#9966CC [IMAGE]
Easter Purple
#CC99FF [IMAGE]
Deep Purple
#330066 [IMAGE]
Grape
#663399 [IMAGE]
Blue Violet
#9966FF [IMAGE]
Blue Purple
#9900FF [IMAGE]
Deep River
#6600CC [IMAGE]
Deep Azure
#6633FF [IMAGE]
Storm Blue
#330099 [IMAGE]
Deep Blue
#3300CC

=20
[<-- Anterior] [Volta para Sum=E1rio]=20

=20
Data da =FAltima atualiza=E7=E3o: September 11, 1995
Quaisquer problemas com este sistema de informa=E7=F5es, por favor
informar ao webmaster@dsc.ufpb.br

-- -+- --
http://www.dsc.ufpb.br/~helder (Acho que homepage, tudo bem)
~^

From: Jo?? S?????
To: wjqs@di.ufpe.br
Subject: !!!!

Teen charged with hacking FAU computer
By CHUCK McGINNES

BOCA RATON- A recently graduated high school senior has been charged with
breaking into the computer system at Florida Atlantic State University's College of Science and Engineering, destroying a professor's electronic mail and transferring files to the internet. Thomas Robert Stromberg, 18, who just graduted from Olympic Heights High School, was arrested Thursday at his home west of Boca Raton. He was charged with two felonies- offenses against intellectual property and offenses against computer users. Investigators from the Florida Department of Law Enforcement and FAU seized a computer and related equipment and material from Stromberg's home at 9596 Lancaster Place. FDLE agents also seized computers from other homes in the Boca Raton area. Additional arrests are expected, FAU Detective Carl "Chuck" Aurin said. The investigation began in February after Elise Angiollilo, FAU's director of tele-communications, discovered someone had gained access to the computers in the science and engineering department. The hackers apparently used the account of a former FAU student to get into the unversity's computer system. Once they had access, they twice tried to crash the computer system and wiped out the electronic mail system of Mahesh Neelakanta, the department's computer system coordinator. Information and copyrighted software from the computer files were transferred to the Internet, where the data could be copied by anyone using the Internet. FAU officials would not say what was in the files.

"The university has very significant information in the computer. The equipment is used by the state for a specific purpose: education and research," said Tom Horton, a computer science and engineering professor. Neelakanta found and FAU computer account that was being used to request information from an outside computer system. The outside system asked for personal information and the individual using the account entered Stromberg's name, according to an arrest report. Stromberg told the police he used a program to crack password files that allowed him into several user accounts where he stored pirated software. This is not the first time hackers have broken into the computer system of a government agency in Palm Beach County, In 1992, a
15-year-old Jupiter boy allegedely tinkered his way into a South Florida Water Management District computer system. Sheryl Woodm a district attorney, said she could not recall if criminal charges were filed against the boy, but she remembered seeing a letter of apology from the youth. Investigators said most hackers break into computer systems for the bragging rights.
They usually write bulletin boards and share the information they obtain with other hackers. Stromberg, who was a member of his school's computer club, went by the name Dr. Jekyll. He is being held at the county jail on $1,000 bail.

LISTA DE PIADAS

To: Multiple recipients of list
Subject: [PIADAS-L] Como desinscrever-se da sub-lista piadas-l do Brasil

Se voce esta' recebendo esta noticia, voce esta' inscrito na
sub-distribuicao Brasil da lista de piadas.

Se voce quiser desinscrever-se desta lista, envie mail para o
endereco listproc@listas.ansp.br, *sem* subject, com uma linha de
comando: unsubscribe piadas-l

Esse e' um servidor automatico, de modo que voce nao podera' falar
livremente como se fosse uma pessoa. Se bem que xingar um
listserver automatico aas vezes desopila... :-]

Se voce quiser contar a alguem como se inscrever, diga para
enviarem mail para listproc@listas.ansp.br com uma linha de
comando:

subscribe piadas-l "Seu Nome Completo"

Por favor, nao envie pedidos de subscribe para a lista, nem para o
pobre do Walter, que ja' nao aguenta mais!

Este mail e' gerado automaticamente todos os dias, para que fique
bem gravado na memoria dos assinantes. Piada, nao?

Virtualmente,
A*e

P.S. para enviar para toda a lista use piadas@psg.com
gerado no dia 12-JUN-1996 22:02:09.39

Sender: piadas@psg.com.nao
From: ???????????@prism.uvsq.fr (???? ??????)
Subject: Evolucao de um programador

Desculpe os nao iniciados, mas esta so' tem graca para quem sabe alguma coisa de programacao:

Iniciante
==========

```
10 PRINT "HELLO WORLD"
20 END
```

Primeiro ano em computacao
==========

```
program Hello(input, output)
  begin
    writeln('Hello World')
  end.
```

No final do curso
==========

```
(defun hello
  (print
    (cons 'Hello (list 'World))))
```

Novo profissional
==========

```
#include
void main(void)
{
  char *message[ = {"Hello ", "World"};
  int i;

  for(i = 0; i < 2; ++i)
    printf("%s", message[);
  printf("\n");
}
```

Profissional esporadico

```
#include
#include

class string
{
private:
  int size;
  char *ptr;

public:
  string() : size(0), ptr(new char('\0')) {}

  string(const string &s) : size(s.size)
  {
    ptr = new char[size + 1];
    strcpy(ptr, s.ptr);
  }

  ~string()
  {
    delete [] ptr;
  }

  friend ostream &operator <<(ostream &, const string &);
  string &operator=(const char *);
};

ostream &operator<<(ostream &stream, const string &s)
{
  return(stream << s.ptr);
}

string &string::operator=(const char *chrs)
{
  if (this != &chrs)
  {
    delete [] ptr;
   size = strlen(chrs);
    ptr = new char[size + 1];
    strcpy(ptr, chrs);
  }
  return(*this);
}

int main()
{
  string str;
```

```
  str = "Hello World";
  cout << str << endl;

  return(0);
}

Programador Master
==================
[
uuid(2573F8F4-CFEE-101A-9A9F-00AA00342820)
]
library LHello
{
    // bring in the master library
    importlib("actimp.tlb");
    importlib("actexp.tlb");

    // bring in my interfaces
    #include "pshlo.idl"

    [
    uuid(2573F8F5-CFEE-101A-9A9F-00AA00342820)
    ]
    cotype THello
 {
 interface IHello;
 interface IPersistFile;
 };
};

[
exe,
uuid(2573F890-CFEE-101A-9A9F-00AA00342820)
]
module CHelloLib
{

    // some code related header files
    importheader();
    importheader();
    importheader();
    importheader("pshlo.h");
    importheader("shlo.hxx");
    importheader("mycls.hxx");

    // needed typelibs
    importlib("actimp.tlb");
    importlib("actexp.tlb");
    importlib("thlo.tlb");

    [
    uuid(2573F891-CFEE-101A-9A9F-00AA00342820),
    aggregatable
    ]
    coclass CHello
 {
 cotype THello;
 };
};
```

```
#include "ipfix.hxx"

extern HANDLE hEvent;

class CHello : public CHelloBase
{
public:
    IPFIX(CLSID_CHello);

    CHello(IUnknown *pUnk);
    ~CHello();

    HRESULT  __stdcall PrintSz(LPWSTR pwszString);

private:
    static int cObjRef;
};


#include
#include
#include
#include
#include "thlo.h"
#include "pshlo.h"
#include "shlo.hxx"
#include "mycls.hxx"

int CHello::cObjRef = 0;

CHello::CHello(IUnknown *pUnk) : CHelloBase(pUnk)
{
    cObjRef++;
    return;
}

HRESULT  __stdcall  CHello::PrintSz(LPWSTR pwszString)
{
    printf("%ws\n", pwszString);
    return(ResultFromScode(S_OK));
}


CHello::~CHello(void)
{

// when the object count goes to zero, stop the server
cObjRef--;
if( cObjRef == 0 )
    PulseEvent(hEvent);

return;
}

#include
#include
#include "pshlo.h"
#include "shlo.hxx"
```

```
#include "mycls.hxx"

HANDLE hEvent;

 int _cdecl main(
int argc,
char * argv[]
) {
ULONG ulRef;
DWORD dwRegistration;
CHelloCF *pCF = new CHelloCF();

hEvent = CreateEvent(NULL, FALSE, FALSE, NULL);

// Initialize the OLE libraries
CoInitializeEx(NULL, COINIT_MULTITHREADED);

CoRegisterClassObject(CLSID_CHello, pCF, CLSCTX_LOCAL_SERVER,
    REGCLS_MULTIPLEUSE, &dwRegistration);

// wait on an event to stop
WaitForSingleObject(hEvent, INFINITE);

// revoke and release the class object
CoRevokeClassObject(dwRegistration);
ulRef = pCF->Release();

// Tell OLE we are going away.
CoUninitialize();

return(0); }

extern CLSID CLSID_CHello;
extern UUID LIBID_CHelloLib;

CLSID CLSID_CHello = { /* 2573F891-CFEE-101A-9A9F-00AA00342820 */
    0x2573F891,
    0xCFEE,
    0x101A,
    { 0x9A, 0x9F, 0x00, 0xAA, 0x00, 0x34, 0x28, 0x20 }
};

UUID LIBID_CHelloLib = { /* 2573F890-CFEE-101A-9A9F-00AA00342820 */
    0x2573F890,
    0xCFEE,
    0x101A,
    { 0x9A, 0x9F, 0x00, 0xAA, 0x00, 0x34, 0x28, 0x20 }
};

#include
#include
#include
#include
#include
#include "pshlo.h"
#include "shlo.hxx"
#include "clsid.h"

int _cdecl main(
int argc,
```

```
char * argv[]
) {
HRESULT  hRslt;
IHello        *pHello;
ULONG  ulCnt;
IMoniker * pmk;
WCHAR  wcsT[_MAX_PATH];
WCHAR  wcsPath[2 * _MAX_PATH];

// get object path
wcsPath[0] = '\0';
wcsT[0] = '\0';
if( argc > 1) {
    mbstowcs(wcsPath, argv[1], strlen(argv[1]) + 1);
    wcsupr(wcsPath);
    }
else {
    fprintf(stderr, "Object path must be specified\n");
    return(1);
    }

// get print string
if(argc > 2)
    mbstowcs(wcsT, argv[2], strlen(argv[2]) + 1);
else
    wcscpy(wcsT, L"Hello World");

printf("Linking to object %ws\n", wcsPath);
printf("Text String %ws\n", wcsT);

// Initialize the OLE libraries
hRslt = CoInitializeEx(NULL, COINIT_MULTITHREADED);

if(SUCCEEDED(hRslt)) {


    hRslt = CreateFileMoniker(wcsPath, &pmk);
    if(SUCCEEDED(hRslt))
 hRslt = BindMoniker(pmk, 0, IID_IHello, (void **)&pHello);

    if(SUCCEEDED(hRslt)) {

 // print a string out
 pHello->PrintSz(wcsT);

 Sleep(2000);
 ulCnt = pHello->Release();
 }
    else
 printf("Failure to connect, status: %lx", hRslt);

    // Tell OLE we are going away.
    CoUninitialize();
    }

return(0);
}
```

Hacker Aprendiz
==========
```
#!/usr/local/bin/perl
$msg="Hello, world.\n";
if ($#ARGV >= 0) {
  while(defined($arg=shift(@ARGV))) {
    $outfilename = $arg;
    open(FILE, ">" . $outfilename) || die "Can't write $arg: $!\n";
    print (FILE $msg);
    close(FILE) || die "Can't close $arg: $!\n";
  }
} else {
  print ($msg);
}
1;
```

Hacker Experiente
==========
```
#include
#define S "Hello, World\n"
main(){exit(printf(S) == strlen(S) ? 0 : 1);}
```

Hacker Ocasional
==========
```
% cc -o a.out ~/src/misc/hw/hw.c
% a.out
```

Hacker Guru
==========
```
% cat
Hello, world.
^D
```

Gerente iniciante
==========
```
10 PRINT "HELLO WORLD"
20 END
```

Gerente
==========
```
mail -s "Hello, world." bob@b12
Bob, Voce poderia me escrever u programa que escreva  "Hello,
world." na tela?
Eu preciso disto para amanha.
^D
```

Gerente Senior
==========

```
  % zmail jim
  Eu preciso de programa "Hello, world." para hoje a tarde.



  Executivo Chefe
  ===================
  % letter
  letter: Command not found.
  % mail
  To: ^X ^F ^C
  % help mail
  help: Command not found.
  % damn!
  !: Event unrecognized
  % logout

 --
 Joao Araujo
```

```
From: A????? M?????????? P??????
Subject: O novo dispositivo de Busca

submeta informatica-jb
O NOVO DISPOSITIVO DE BUSCA

Um novo dispositivo de busca chamado Hotbot utiliza "hive computing"
(computacao em colmeia) que conecta varias estacoes de trabalho em uma
rede de tal modo que cada maquina pode trabalhar em uma parte separada
da busca das quase 50 milhoes de paginas existentes agora na World Wide
Web.  Uma versao beta publica se encontra no endereco:
< http://www.hotbot.com >

New York Times 21 mai 96 C5
```

```
From: ????? ?????
To: java-l@di.ufpe.br
Subject: Um furo na seguranca do Java

Oi pessoal,

Peguei essa noticia na parte de infomatica do Brasil OnLine. Eu como todos
voces, tambem espero que seja resovido logo.

"Um pesquisador ingljs descobriu um furo na seguranga da linguagem Java que
permite  que  usuarios  manipulem alguns objetos e  enganem  o  sistema  de
seguranga.  O  pesquisador,  David Hopwood, diz em seu  site  na  Web  que,
explorando  um  bug no mecanismo que separa as classes  JVM  (Java  Virtual
Machine)  em diferentes nomes e espagos, um programador pode  passar  ileso
por  todas  as restrigues de seguranga, incluindo a leitura  e  escrita  de
arquivos e a execugco de csdigo nativo no cliente com as mesmas  permissues
do usuario do navegador.

Segundo  Hopwood, o furo ss pode ser consertado atravis do desligamento  do
```

Java. O problema afeta todos os navegadores atuais que suportam a linguagem. David ja informou sobre o bug ` JavaSoft, subsidiaria da Sun Microsystems Inc., de Mountain View, Califsrnia, que desenvolve, distribui e da assistjncia ` linguagem. Segundo o site da JavaSoft na Web, um grupo esta trabalhando no problema e conduz tambim uma revisco geral na seguranga do Java em busca de bugs semelhantes. O site de Hopwood pode ser acessado em http://ferret.lmh.ox.ac.uk/~david/java/bugs/."

Abracos,

D???? C????
e-mail: ????@???????.???.br

BIBLIOGRAFIA

O artigo sobre UNIX nem vou responder. Pura experiencia e leitura de varios manuais, incluindo uma apostila "XENIX 1-2-3".

O lance sobre esconde-esconde e' uma parte fruto da minha infancia, parte d adolescencia e ultimas vivencias em comunidade, alem de leituras de artigos de jornais e filmes variados.

Algumas das noticias, acho ate' que todas, foi contribuicao de algumas pessoas que prefiro nao colocar o nome. Elas podem nao gostar..

Algumas das dicas, eu peguei no Netsurf, uma dica do Morpheus.
Nao sei se ainda rola este e-zine, mas fica a referencia:
Netsurfer Focus Home Page: http://www.netsurf.com/nsf/index.html

A dica do snoop, foi do jornal ESTADO DE SAO PAULO 8/07/96, folha de informatica.

As piadas, garimpo todas na lista de piadas, ate' coloquei a carta pra quem quiser se subscrever, mas aviso: sao as vezes cerca de 30 a 50 por dia.

O artigo sobre BBSes que nao estao no mapa, eu tirei a ideia de outro que nao tive a paciencia pra traduzir. Final de semestre, nao devia nem estar editando o Barata Eletrica. Nao adianta tambem se oferecer p. traduzir, muito menos pedir o dito.

DIAL-A-VIRUS REVISITED: THE CREEPING EVIL OF PRIVATE BULLETIN BOARDS CONTINUES TO SAP AND IMPURIFY OUR PRECIOUS BODILY FLUIDS
Computer Virus Developments Quarterly
(American Eagle Publishing, Tucson, AZ)