BARATA ELETRICA, numero 2
Sao Paulo, 23 de marco de 1995

Conteudo:

Creditos:

Este jornal foi escrito por Derneval R. R. da Cunha
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. Aqueles interessados em receber futuras edicoes deste ou de outro jornal (nao sei se ira' continuar com esse titulo) mandem um mail eletronico para: wu100@fim.uni-erlangen.de

INTRODUCAO:
==========

Devido ao que aconteceu aqui na USP, resolvi mais uma vez publicar um texto sobre o que eu acho que os hackers sao.

Texto da revista ZAP! 23 de outubro de 1994 - Jornal ESTADO DE SAO PAULO

O que e' um hacker? Nao existe traducao. A mais proxima seria "fussador" e o verbo to hack, "fucar". Hacker, vulgo "rato de laboratorio", era o termo usado pelos estudandes

do MIT para designar aqueles que"fucavam" nos computadores da Universidade alem dos limites de uso. O Hacker difere do Guru, que ja' sabe tudo. Ele quer e' descobrir como mexer com tudo (o contrario do usuario comum, que nao tem remorso de usar um micro Pentium para escrever cartas durante o expediente). Nao teme virus de computador. O interessante ate' seria escrever um, mas nao para difundir, so' exibir p\ colegas. Infelizmente, o filme "Wargames", estimulou muitos adolescentes a tentar seguir o exemplo, chegando no chamado vandalismo eletronico e acabaram sendo presos por isso com grandes manchetes nos jornais denegrindo o termo. Ao contrario de outros, como Mitch Kapor, que deu aulas de meditacao transcendental durante anos, ate desistir e comprar um Apple. Tempos depois seria dono da Lotus(1-2-3). Houve agora, em Buenos Aires, durante os dias 7,8 e 9, o primeiro Congressso Internacional de Hackers e fabricantes de Virus da America Latina. O evento foi organizado por Fernando Bomsembiante, diretor da revista argentina de Hackers "Virus Report". Varias personalidades, como Goldstein, editor da revista 2600, referencia basica para este universo, Patrice, editor da revista holandesa Hack-Tic, tambem realizador de um congresso de Hackers, estiveram presentes e Mark Ludwig, autor de "Computer Viruses, Artificial Life and Evolution" e especialistas argentinos. Houve discusses e palestras sobre cultura Cyberpunk, Multimidia, Auditoria Bancaria, e varios assuntos ligados a Cibernetica. A ESCOLA DO FUTURO, Instituto ligado a Pr-Reitoria de Pesquisa da USP participou com uma palestra sobre Ensino a Distcncia. O pblico era composto em sua maioria de adolescente, com varios profissionais liberais da area de educacao e donos de BBSes argentinas. Os hackers argentinos nao se deixam fotografar, usando ate um jato de extintor de incendio para coibir tentativas, apesar da inexistencia de legislacao sobre a atividade na Argentina. O encontro foi um grande sucesso de pblico, que ja contava com reunioes na primeira semana de cada mes.

MAIS UM POUCO DE HISTORIA..

Continuando com o saudosismo do numero anterior. Compare a situacao da sua faculdade com o que eu passei em outra. Ou passe para a outra materia.

Quando eu estava estudando para o vestibular, o quente no cinema era o filme "Wargames" e o quente na TV era o MSX-Hot Bit da Sharp. O mais legal era poder escrever direto na tela do micro, com uma caneta especial. Isso era disponivel no TK90, se nao me engano.

Na epoca, estava com 19 aninhos e ouvi, enquanto estava peruando numa loja de informatica num shopping do Rio de Janeiro:
- Pois e', fulano comecou na informatica com um daqueles micros de 2 bits, um dos primeiros que chegaram aqui no Brasil. Depois passou para um de 8 bits, os pais resolveram investir e agora com 15 anos, ele tem um escritorio de venda de programas.

Naquele tempo so' existia o Basic e a linguagem de maquina como

opcoes para desenvolvimento de software comercial. Acho que era possivel usar outras linguagens, mas isso consumia mais memoria.

Em 1987, entrei para uma Universidade famosa em Sao Paulo por suas greves e reacao ao governo militar. Nao por causa disso, era uma das poucas opcoes para bacharelato em computacao. Tambem era famosa pelo alto indice de desistencia, o ESTADO DE SAO PAULO soltou uma materia comentando acho que 20000 pessoas desistindo de pagar as altas mensalidades. Ficar na secao de alunos dela era ouvir historias fantasticas de ma' contabilidade financeira, perda de dados e esperas fantasticas para ouvir negativas impossiveis e injustas. Mantenho em segredo o nome. O lema do cara la' dentro era: "Estude, do contrario voce vai repetir essa mesma m(*) o ano que vem". A turma de computacao da faculdade de exatas tinha um ano. Cinquenta por cento do pessoal ia direto para a quadra de basquete durante as aulas de Calculo I. A materia "Introducao a Computacao" era dada com micros Apple][recem comprados. O pessoal achava uma inovacao, pois no ano anterior, a materia era dada sem micros de qualquer especie e com linguagem BASIC.

Tem gente que pode achar, PO, nao to com saco p. ler sobre isso. Tudo bem, mas um dia voce vai para uma faculdade e ai' podera' reler isso aqui e saber que apesar da condicoes horripilantes, voce pode acabar chegando a aprender alguma coisa. Principalmente se mudar para uma faculdade que preste.

A FATEC de Sao Paulo era pior. As aulas eram feitas com COBOL. O computador de la' era uma reliquia dos primeiros tempos da computacao. Ja' ouviu falar de cartao perfurado? Isso existia. Algumas escolas tecnicas de segundo grau ainda usavam dar aula de Pascal com esse tipo de computador. Ou como diz o ditado: A sua experiencia cresce na razao inversa a qualidade do equipamento que voce utiliza. O pior e' que naqueles anos, a maioria dos anuncios pedindo estagiarios tambem pediam como pre-requisito o conhecimento de COBOL.

Pelo que eu me lembro havia a famosa reserva de mercado. Isso significava basicamente que, havendo similar nacional, o produto externo nao tinha concorrencia ou mesmo entrada aqui no Brasil. Se a pessoa conseguisse demonstrar "in paper" a necessidade de um Macintosh, ela poderia comprar um. Com sorte, em alguns meses toda a papelada estaria terminada e a alfandega liberaria o micro. Todo mundo era obrigado a comprar somente o que era produzido no Brasil. Que, como nao tinha lei de protecao ao consumidor, ficava obrigado a engolir umas porcarias, tipo o famoso Solution 16.

Esse dai foi um micro, XT, que entrou no mercado como o mais barato de todos. Era barato porque os primeiros nao funcionavam. Uma jornalista comprou, e teve que gastar um dinheiro enorme em cursos de informatica para descobrir que, independente de usar software legitimo, independente de conhecimentos de informatica, o micro nao funcionava. Teve certeza disso quando ao fazer uma materia com um alto funcionario da empresa. Este confirmou que o micro que ela comprou, para funcionar, teria que ser reconstruido, e que a empresa sabia disso, mas nao avisou ninguem por medo das consequencias negativas do fato. Ela contou sua odisseia numa materia que escreveu para uma revista dessas de jornal de domingo.

Durante o ano e meio que fiquei naquela porcaria de Universidade, entrei em contato com varios tipos de software pirateado. Havia um culto a pirataria, naqueles tempos, com um programa chamado Locksmith, sendo muito procurado para copiar software em Apple. Me lembro de ter comprado ate' um livro, publicado por um brasileiro (na veradade escrito por ele) chamado "Dicas e Truques do Locksmith". Explicava todos os truques para se proteger e desproteger disquetes. Outro software muito usado, em PC, eram o Copy II - PC e o Copywrite, da Central Point. Nao, eu mesmo nunca travei contato com esses softwares, mas sei de muita gente que nao teria aprendido a usar Lotus 1-2-3, DBASE III + ou Word sem eles.(Tudo bem, admito algo mais do que um contato).

Ha' pouco tempo encontrei um ex-conterraneo. Tinha se formado, e estava de saco cheio de informatica. Resolveu fazer Letras-Alemao para desanuviar a cabeca e parar de mexer com algoritimos. Depois que a pessoa

se forma, ela passa a falar bem da Instituicao que lhe deu o diploma. Quando sai daquela, havia um aumento de 1400 % sobre o preco para se fazer a matricula. Durante o tempo em que fiquei la' poderia dizer que houve um aumento de 100 % ao mes, e haviam 8 ou 10 XTs e 3 ou 4 apples funcionando para toda a faculdade de Matematica, Computacao e Estatistica praticarem. Mais de 300 pessoas. Estremeco, so' de pensar o quanto se paga hoje em dia, para se graduar em informatica.

PIRATA ELETRONICO INVADE ARQUIVOS DA USP

Condensado da materia do
Estado de Sao Paulo - 23-2-95 - Neide Maria Silva

Sao Carlos - A onda dos hackers, os piratas eletronicos que se divertem descobrindo senhas que dao acesso a arquivos de computacao, chegou semana passada a Universidade de Sao Paulo. O primeiro departamente a ter parte de seus arquivos apagadosfoi a Engenharia Eletrica, na terca-feira. No dia seguinte, o ataque foi na Fisica, que perdeu informacoes armazenadas em tres discos e ficou com uma importante estacao de trabalho parada seis horas. Audacioso, o hacker entrou tambem com sucesso nos sistemas do Departamento de Matematica, na quinta-feira.

A acao foi considerada como "uma brincadeira maldosa", ja' que o hacker nao teve nenhum proveito pratico com o ataque. O assunto foi mantido em sigilo para evitar atrair a atencao de outros genios ciberneticos. Segundo o professor Jan Slacts, responsavel pelo servico de informatica do Departamento de Fisica, a invasao comecou por volta das tres horas da madrugada e o hacker chegou a pedir aos usuarios que estavam no sistema para que avisassem o FANTASTICO sobre o que ele estava fazendo.

[Parte editada - sem saco para digitar]

Precaucao - Esta nao e' a primeira vez que um pirata eletronico invade os computadores da USP de Sao Carlos. No ano passado, um estudante da fisica se divertiu durante varios dias quebrando as senhas dos usuarios a partir de um terminal da sala de alunos. O pirata foi apanhado e agora enfrenta um inquerito na escola. "No caso desse aluno, foi uma brincadeira de adoles cente que nao causou nenhum prejuizo; e' diferente do que houve agora, porque esta foi uma acao muito bem informada", comentou Slacts.

Para tentar evitar novas invasoes, a USP de Sao Carlos esta' colocando barreiras para impedir o acesso externo a rede e melhorando o sistema para que o material apagado possa ser recurperado em menos de 15 minutos.

EFEITOS COLATERAIS NO BARATA ELETRICA

Na terca-feira, a coluna Netvox, do Jornal FOLHA DE SAO PAULO, comentou a existencia do Barata Eletrica, como o primeiro Hacker E-Zine Brasileiro. Isso, logo apos o "break-in" no computador da USP em Sao Carlos.

Todo computador ligado a Internet tem a sua equipe de Sysops ou "Super-Users", encarregados de fazer a manutencao e controlar o acesso a maquina. O encarregado da maquina onde eu tinha a conta que foi anunciada no jornal congelou o acesso a minha conta, ate' que eu aparecesse para explicar o quais eram minhas intencoes. Tive que explicar que minha preocupacao era sobre hacking e nao cracking (ver texto abaixo).

"A Internet esta' comecando a explodir no Brasil. As pessoas terao que discutir isso em Rede, um dia. Eu nao estou ensinando o mal caminho".

Mesmo assim, como havia uma especie de caca as bruxas, ele me pediu para arrumar outra forma de manter minha lista eletronica. No meu local de trabalho, tambem me falaram quase a mesma coisa. "O problema sao as macas podres", Derneval.

Mais interessante foi quando enviei para rede uma mensagem comunicando que aquela poderia ser a ultima (exagerei). Recebi duas cartas, uma me chamando nao de "Bode expiatorio", mas de "Burro expiatorio", ja' que deveria esperar retaliacao por tal atitude "rebelde" e uma outra, mais simpatica, concordando que eu era ingenuo em "chorar" esse tipo de atitude.

Isso e' o que se chama de "flame". Alguem solta uma coisa extremamente ofensiva para gerar discussao. Gerou. Doeu, foi chato (nao esperava). Algumas pessoas, a par do problema deram o maior apoio moral e uma ofereceu ajuda. Apesar de coisas estranhas, (tipo cair a sessao umas duas ou tres vezes quando eu editava o dito), a gente vai levando.

Todo esse trabalho ainda vai valer a pena, se essa ideia vingar:

Colocar um monte de caras viciados em micro, mais ou menos com experiencias e problemas semelhantes aos que ja' passei, numa sala, trocando historias, dicas e quem sabe progredindo em conjunto, passando adiante experiencias. E se a conversa esbarrar em "Computer Underground", tudo bem. Tem muita gente que conversa sobre guerras, matar gente, roubo de bancos. Nem por isso saem por ai' cometendo crimes. As pessoas que tiverem esse tipo de motivacao para o mal, irao descobrir que o esforco nao compensa.

CRIME POR COMPUTADOR

Em virtude dos ataques ocorridos na USP, resolvi trazer esses arquivos, tirados da revista NIA, como mostra abaixo. Ia traduzir, adaptar, mas.. achei melhor deixar estas partes selecionadas do original para ajudar a mocada a treinar seu ingles.

:_Computer Crimes/Fraud/Waste part 1 - N.I.A.
:_Written/Typed/Edited By: Lord Kalkin

When Computers were first introduced, few were available and only a small number of persons were trained to use them. Computers were usually housed in seperate, large areas far removed from programm managers, analysts, economists, and statisticians. Today that is changed. Word processors, computer terminals, and desktop computers are as common equipment. This electronic equipment is rapidly becoming increasingly user-friendly so that many people can quickly and easily learn how-to use it.

Employees with access to computer equipment and automated information are greatly increasing throughput the organizational hierachy. The GS-4 secretary, the GS-9 budget analyst, the GS-12 program analyst, the GS-13 statician, the GM-14 economist, and the Senior Executive Service Manager may have all the access to a computer terminal or word processor and the information it contains.

No longer is information restricted to select few at the highest levels of an organization. This phenomenon has led computer crime to be called the "democratization of crime." As more people gain access to automated information and equipment, the opportunities for crime, waste, and abuse likewise increase.

It's Difficult to Generalize, But...

- Functional end user, not the tecnical type and not a hacker

- holds a non-supervisory position
- no prevoius criminal record.
- bright, motivated, desirable employee
- works long hours; may take few vacations
- Not sophisticated in computer use
- The last person YOU would suspect
- Just the person YOU would want to hire

THE COMPUTER CROOK CAN BE ANYONE

The typical computer crook is not the precocious hacker who uses a telephone and home computer to gain access to major computer systems. The typical computer crook is an employee who is a legitimate and nontechnical end user of the system. Nationally, employee-committed crime, waste, and abuse account for an estimated 70 to 80 percent of the annual loss related to computers. Dishonest and disgruntled employees cause an estimated 20 percent of the total computer system related loss. And they do so for a variety of reasons.

WHY PEOPLE COMMIT COMPUTER CRIME

- Personal or Financial gain
- Entertainment
- Revenge
- Personal Favor
- Beat the system, Challenge
- Accident
- Vandalism

But a significantly lager dollar amount, about 60 percent of the total computer-related loss, is caused by employees through human errors and accidents. Preventing computer losses, whether the result of debliberately committed crimes or unknowingly caused waste, requires security knowledge and security awareness. A recent survey reported that observant employees were the primary means of detecting computer crime.

CLUES TO COMPUTER CRIME ABUSE

Be on the look out for...

- Unauthorized use of computer time
- Unauthorized use of or attempts to access data files
- Theft of computer supplies
- Theft of computer software
- Theft of computer hardware
- Physical damage to hardware
- Data or software destruction
- Unauthorized possession of computer disks, tapes or printouts.

This is a beginning list of the kinds of clues to look for in detecting computer crime, waste, and abuse. Sometimes clues suggest that a crime has been committed or an abusive practice has occured. Clues can also highlight systemn vunerabilities -- identify where loopholes exist -- and help identify changes that should be made. Whereas clues can help detect crime and abuse, conrols can help prevent them.

Controls are management-initiated safeguards -- policies or

administrative procedures, hardware devices or software additions -- the primary mission of which is to prevent crime and abuse by not allowing them to occur. Controls can also serve a limitation function by restricting the losses should a crime or abuse occur.

This document addresses information security into three areas: Information Secrurity, Physical Security, and personnel security. In each area, crimes, clues, and controls are discussed. In these areas not only frauds, but abuses and waste are addressed. The final chapters provide a plan of action and cite availably security resources.

N.I.A. - Ignorance, There's No Excuse.
Founded By: Guardian Of Time/Judge Dredd.

[Observacao: alguns paragrafos do texto foram retirados para maior clareza]
[OTHER WORLD BBS]
/

O CRIME DE COMPUTADOR E A
LEGISLACAO BRASILEIRA ATUAL
==========

Coletanea de artigos de Direito e Informatica publicados em Jornais e Revistas, abordando os mais variados temas sobre informatica e sua legislacao especifica, aspectos tributarios, trabalhistas, bem como protecao de direitos autorais.

Os artigos sao assinados por MARCOS WACHOWICZ, Professor das Faculdades Positivo, Mestre em Direito pela Universidade Classica de Lisboa - Portugal, Pos-Graduacao em Filosofia do Direito e Didadica PUC - PR, especializado na area de direito e informatica.

E' permita a reproducao total ou parcial desde que mencionada a fonte, autoria e sinopse do autor.

##
As acoes civeis e penais contra a pirataria.
##

O titular dos direitos autorais do programa de computador, seja pessoa fisica ou juridica, podera recorrer a medidas judiciais contra terceiros que utilizem ou reproduzam ilegalmente o programa, isto independentemente da finalidade da reproducao ilegal (copia pirata) ser ou nao comercial.

O desconhecimento dos procedimentos legais aliada # id#ia gen#rica de que o processo judicial sempre sera moroso, faz com que muitas vezes nao se recorra ao Poder Judiciario na defesa dos direitos autorais violados pela pirataria.

Por#m, ao contrario a legislacao de informatica, instrumentalizou o tramite processual das acoes contra a pirataria e com#rcio ilegal de software, com medidas liminares, ou seja, antes do julgamento da acao, podera o titular dos direitos autorais lezados coibir a pratica da pirataria, bem como o infrator se sujeitar a multa pecuniaria diaria.

Para que seja acionado o Judiciario # imprescindivel que o titular dos direitos autorais possua prova cabal da titularidade do software. Isto atrav#s de registro no INPI.-Instituto Nacional de Marcas de Patentes, ou compravada comercializacao do produto com

o registro no SEI. - Secretaria Especial de Informatica.

O primeiro passo a ser dado ent#o sera a notificacao judicial da pessoa fisica ou juridica que estiver de posse do software pirata, para que se abstenha da pratica de reproducao, e ainda, destrua a copia ilegal.

Na pratica verifica-se que uma vez realizada a notificacao muitas empresas deixam de utilizar a copia pirata, procurando a empresa produtora para aquisicao do programa que antes utilizavam ilegalmente.

Caso a notificacao nao surta esse efeito regularizador - que # o ideal -, posto que nao implica de imediato na abertura de inqu#rito policial, nem de acao civel indenizatoria , havera ent#o, o segundo passo ha ser dado, que seria o ingresso de acoes penais ou civeis a crit#rio da parte lezada.

A instauracao de inqu#rito policial para apurar o crime deve ser solicitada pela parte detentora dos direito autorais dos programas. O inqu#rito pode ser tanto contra o usuario de um software pirata, como tamb#m contra as empresas de revenda que comercializem ilegalmente.

No mes de marco/93, as Empresas Audesk, Lotus, Microsoft, Novell e Wordperfec, receberam denuncia de irregularidade nos produtos comercializados pela empresa paulista All Soft. Em diligencia preliminares foi verificada a inexistencia de registro desta empresa na Junta Comercial.

Em seguida, mediante acao penal propria, foi autorizado judicialmente que policiais e t#cnicos da 4a. Delegacia do DEIC., realizassem o flagrante e procedessem a apreensao dos programas piratas, que ser#o objeto de analise dos peritos da Criminalistica da Policia Civil. Caracterizou-se, mais ainda a revenda ilegal pelo fato foram apreendidos centenas disquetes e cerca de 1.000 folhetos de propaganda. Al#m disso, foram recolhidos 3 computadores e 1 impressora que nao possuiam nota fiscal de compra.

Um paralelo com a Legislacao Argentina # oportuno, pois, em casos analogos, a Justica apreende todo material encontrado, a propaganda, os disquetes, e os computadores. No Brasil, a legislacao # mais branda, o perito recolhe as evidencias de que havia copia pirata nos micros, confiscando apenas os disquetes.

Assim, no caso supra mencionado os 3 computadores e a impressora somente foram apreendidos por suspeita de contrabando de hardware, e nao por forca da medida judicial que visava proteger os direitos autorais de software.

Independentemente da instauracao do inqu#rito podera o titular dos direitos autorais interp#r na esfera civel medidas cautelares e indenizatorias.

A Lei de Informatica preve a medida cautelar civel de busca e apreensao cominada com pena pecuniaria diaria no caso de pirataria ou no descumprimento da ordem judicial.

Vale dizer: o juiz no primeiro despacho podera

conceder liminarmente a busca e apreensao das copias piratas, ato que se realizara atraves de diligencias do Oficial de Justica, peritos e forca policial se necessario. Isto sem que se analise o m#rito da acao.

A multa diaria # estipulada livremente pela parte titular dos direitos autorais, em face dos prejuizos que o transgressor lhe causar, podendo pois, o Juiz ao seu livre arbitrio e conviccao majora-la ou reduzi-la conforme sua analise sobre o caso.

A fixacao da multa sera concomitante com o despacho inicial concessivo da liminar, que # o despacho inicial do processo.

O infrator mesmo que se abstenha da pratica do ato lesivo, com o intuito de nao lhe ser imputada multa diaria, mesmo assim, ao final do processo com a prolacao da sentenca, o juiz podera fixar indenizacao por perdas e danos desde que seja tal pedido cumulado na inicial.

Inobstantemente #s perdas e danos, o titular do direito autoral lesado, podera at# promover acao ordinaria de indenizacao por danos morais, caso se verifique os prejuizos de ordem imaterial que est#o ligados ao bem juridico tutelado.

O prazo prescricional das acoes civeis e penais por ofensa a direitos patrimoniais do autor foi fixada em 05 (cinco) anos (Lei 7.646/87). Contudo, entendemos, que tal prazo, # dispare considerando que, a mesma Lei, fixa a protecao dos direitos autorais sobre o software em 25 anos. E, ainda, no direito civil tem como base prescricional das acoes ordinaria o prazo de 20 anos.

MARCOS WACHOWICZ, # advogado especializado na area de direito e informatica.

##
Crimes cometidos atrav#s do computador
##

Os computadores entraram na vida cotidiana das pessoas e se instalaram na vida moderna nos negocios, nas escolas e tamb#m nos lares numa velocidade de avanco tecnologico e de dissiminacao de produtos impares em toda a historia da civilizacao.

Basta comparar que na ciencia m#dica qualquer elaboracao de vacina e seu efetivo uso pela populacao, transcorrem 10 ou 15 anos, enquanto na area da informatica, seja hardware ou software este tempo entre o desenvolvimento e a comercializacao se reduz nao raras vezes a 1 ou 2 anos.

As relacoes sociais, como tudo o que diz respeito # vida dos homens interessa e # objeto de analise pelo direito, nao podendo este ficar alheio especialmente ao que afeta ao direito comercial e penal.

A utilizacao indevida do computador com fim delituoso (computer by crime), vem crescendo assustadoramente # nivel mundial.

Nos Estados Unidos onde este assunto ja vem analisado com maior rigor, estimou-se que na d#cada de 80, somente 20% (vinte por cento) dos crimes de computador foram efetivamente apreciadados pelos Tribunais, e destes apenas 3% (tres por cento) acabaram condenados.

A raz#o da pouca procura do Poder Judiciario pelas partes lezadas e do infimo indice de condenacao se deve a alguns fatores. Primeiro porque o perfil dos criminosos do chamado "computer by crime" sao de maneira geral jovens cuja idade varia de 17 # 21 anos na Europa, e nos EUA., essa faixa etaria baixa para 12 # 16 anos, o que os torna inimputaveis perante a lei.

Em segundo, porque alguns "computer-crime" nao objetivam vantagens econ#micas ou ganhos financeiros, isto porque, devido ao alto nivel intelectual do criminoso, que apos um certo tempo de contato, de trabalho com o software ou via moldem com outros sistemas de computador, passa a querer desafia-los, surgindo uma esp#cie de "competicao tecnologica" entre a maquina (computador) e o homem (desafiante), numa "disputa ludica" ou "jogo". Dai o porque, de muitos criminosos acharem que nao est#o cometendo ilicito algum, muito menos na ordem criminal.

Disto decorrem uma s#rie de crimes cometidos, como abusos de utilizacao de computador, entradas indevidas em sistemas, que nao raras vezes danificam e tornam inoperantes os programas, acarretando prejuizos elevadissimos #s empresas ou instituicoes . Vitimas que por vezes, preferem nao divulgar suas falhas ou facilidades de acesso, preferindo uma definicao a nivel de administracao interna.

O terceiro tipo poderia ser classificado como "criminoso de colarinho branco", cuja inteligencia e educacao est#o acima da m#dia, gozam de bom conceito entre os demais, trabalham al#m da jornada diaria de trabalho, normalmente sem supervisao, partem para o cometimento de infracoes como copias de programas, vendas a terceiros (inclusive competidores da empresa), emitem ordens de pagamentos, cheques, dividendos de acionistas, lancamentos indevidos. Ressalte-se nessas operacoes nao ficam provas materiais, vestigios que permitam chegar aos criminosos, ja que nao ha interferencia do ser humano, maquina para maquina e a operacao se concretiza.

Esta modalidade # bastante comum nos casos de estelionato e fraudes bancarias ou cartoes de cr#dito com terminais em lojas e comercio (supermercados, restaurantes, etc.), tamb#m nao raras vezes a empresa vitima procura uma solucao interna, sem recorrer ao judiciario temendo pela repercussao negativa do crime do qual foi vitima junto a sua clientela.

Por outro lado, quanto o infimo indice de condenacao pelo Poder Judiciario com relacao aos crimes cometidos atrav#s de computador se deve a outros fatores.

Em tese dentre o elenco de crimes que podem ser cometidos diante da sistematica do nosso Codigo Penal tipificados encontram-se , a violacao de segredo comercial ou profissional, a falsificacao de documentos publicos ou particulares, os crimes contra a inviolabilidades de correspondencia, a sabotagem, o vandalismo, a apropriacao de dados, sendo o estelionato o mais comum.

Contudo, a utilizacao indevida do computador em todas as suas condutas delituosas extrapola em muito os limites

atualmente existentes que permitem o enquadramento penal.

A fase de investigacao, descoberta, apurac#o e a fase probatoria do processo judicial # lenta se comparada a "trama" utilizada pelo agente criminoso. Na medida em que, se o agente criminoso suspeitar ou saber de esta sendo realizada uma sindicancia, podera imediatamente tendo acesso ao computador dar uma ordem a este, dentro da programacao, deletando provas que poderiam lhe ser incriminadoras.

A complexidade de sistemas de coputadorizacao nao so dificultam que as proprias vitimas descubram o golpe, como impedem mais ainda a obtencao de provas para a Justica. Os funcionarios da Policia, os judiciais, membros do Minist#rio Publico e da Magistratura tem dificuldades em deslindar a "trama" utilizada pelo agente, se a fase probatoria se encontrar cercadas de duvidas e incertezas.

A falta de legislacao especifica # um entrave nao so no Brasil, posto que se depara com uma criminalidade do futuro.

Em varios paises Europeus a Scotland Yard investiga uma quadrilha que esta vendo nos patios de escolas, discos opticos do tipo CD-ROM para armazenar e difundir imagens pornograficas entre menores, a precos equivalentes a menos de US$ 1,00. Al#m disso, qualquer menor que tenha em casa um computador com modem, pode acessar a muitos bancos de dados que oferecem imagens pornograficas, #s vezes animadas. Esta # a modalidade de delito # dist#ncia, na qual o agente realiza uma conduta delituosa e, dada a programacao a propria maquina de tempos em tempos repete essa mesma conduta automaticamente. A legislacao Inglesa datada de 1959 nao previa o surgimento da "pornomatica". Os entraves juridicos se acentuam quando se indaga se a competencia de qual Estado para julgar os crime cometidos # dist#ncia, o agente esta em um pais, o sistema de computadores em outro. At# o primeiro- ministro Brit#nico chegou a assumir no inicio do mes de maio, o compromisso de tomar medidas urgentes para reforcar a legislacao contra o "computer by crime".

MARCOS WACHOWICZ, # advogado especializado na area de direito e informatica.

##
O Direito a privacidade e a informacao de dados
##

A Constituicao Brasileira reconhece aos cidad#os direitos fundamentais como de tomarem conhecimento dos dados pessoais introduzidos em computador, de exigirem que sejam retificados e atualizados (se for caso disso), e de saberem o fim a que os dados se destinam.

Os direitos constitucionais objetivam impedir que o cidad#o tenha a sua vida particular totalmente devassada.

Por#m, # certo, que a computadorizacao de servicos em varias esferas de atividade, podem, nao raras vezes possibilitar a invasao da privacidade. Isto atrav#s do cadastro do documento de identitade (Registro Geral, Passaporte), controle fiscal (atrav#s do Imposto de Renda), dados cadastrais (bancarios,cartoes de cr#dito), todos dados armazendos em computadores, que podem ser a qualquer momento, mediante um codigo, serem acionados e totalmente devassados.

Na Espanha ocorreu o esc#ndalo da empresa de publicidade "Publigest", a qual possuia informacoes detalhadas em computador, sobre 21 milhoes de espanhois. Lembre-se que a populacao espanhola # de aproximadamente 45 milhoes de habitantes. Segundo fontes policiais, era a maior base de dados e a melhor documentacao existente. A empresa obtinha dados por meio de uma operacao elementar: cruzava-os. Com o resultado dessa aplicacao obtinha perfis individuais incluindo informacoes sobre rendimentos, nivel cultural, padr#o de consumo, matricula de automovel, e, at#, dados referidos "se#oras con amantes".

Como agia a empresa "Pulbigest" para possuir esta incrivel base de dados? E com que finalidade? Primeiro, contava com cumplicidades nas Administracoes Publicas e Privada. Em segundo, oferecia os seus registros para clientes muito interessados na expansao de seus negocios via publicidade dirigida.

O caso "Publigest" foi levado aos Tribunais. A principio foi determinada a prisao dos diretores da empresa. Contudo, logo em seguida, foi determinada a libertacao. Isto porque, ficou patente a lacuna legal dos delitos imputados aos detidos. Ou seja, acumular uma s#rie de dados privados sobre cidad#o nao estava tipificado como um ilicito na Legislacao Espanhola.

O que # relevante, e este caso demonstrou, # que a informatica descentralizou, se miniaturizou, permitindo que seus suportes sejam verdadeiros "objetos nomades", capazes de grandes performaces, permitindo a disseminacao de bases de dados (gen#ricos e especificos) de forma incontrolavel pela legislacao em vigor.

O Governo espanhol se apressou em enviar uma proposta legislativa ao Parlamento para regulamentar estas questoes.

O mesmo ocorreu com Portugal, que atrav#s de Resolucao do Conselho de ministros, n. 48/92, tratou de forma firme a quest#o do prolema da seguranca juridica dos dados da administracao publica, visando uma garantia efetiva dos direitos do cidad#o.

Alguns principios da Legislacao Portuguesa merecem destaque:

- Principio relativo ao recolhimento, qualidade e tempo de conservacao dos dados: os dados devem ser recolhidos de forma licita e nao enganosa. Devem ser exatos, atuais e suficientes e nao excessivos. E nao devem ser conservados al#m do que seja necessario tendo em conta a finalidade do ficheiro.

- Principio relativo a criacao dos ficheiros: a Lei reafirma a proibicao de tratar em computador os dados relativos a vida privada (art. 35 da Constituicao Lusitana), dispondo a necessidade de lei, para a criacao de banco de dados ligados ao servico publico, bem como, para os eventualmente criados pelo setor privado, a obrigatoriedade de comunicacao # autoridade competente.

- Principio relativo ao processamento de dados: os dados devem ser utilizados apenas para o fim que motivou a sua criacao. Os perfis de personalidade construidos no computador nao podem ser cruzados.

- Direitos da pessoa titular dos dados: a pessoa tem o direito de ser informada sobre os bancos de dados onde existem informacoes que lhe respeitem. Tem direito de acesso, de retificacao, de completar, de suprimir, de queixa, de reclamacao e de recurso. Pode, com vista # defesa desses direitos utilizar a acao civel, medidas cautelares ou a acao penal.

No Brasil, embora exitam preceitos constitucionais que garantam a privacidade e o direito de informacao dos dados armazenados, falta a necessaria mediacao legislativa para tornar operativos esses direitos.

A invasao da privacidade do individuo, a sua intimidade e, at#, no seu direito de estar so, direito do silencio. Necessita, de um aperfeicoamento do ordenamento juridico existente no pais, a exemplo da evolucao havida, especialemente no ambito dos paises da Comunidade Econ#mica Europ#ia (CEE.), com estudos e legislacoes recentes.

MARCOS WACHOWICZ, # advogado especializado na area de direito e informatica.

O HACKER COMO MAU ELEMENTO

Muita gente nao entendeu direito como eu me envolvi nesta historia. Que que eu tenho a ver com a invasao de um computador em Sao Carlos para ter minha conta bloqueada ate' explicar tudo? Resposta: eu criei uma listserv informal me referindo a hackers e material do Computer Underground.

Mas so' isso? E' preciso enxergar isso desde o principio. Apos o filme "Wargames", que mostra um jovem acessando computadores do sistema americano de defesa e quase detonando a terceira guerra mundial (naquele tempo essa possibilidade ainda existia), muita gente quis sentir na boca esse gosto de poder.

Na epoca, os CDFs de computacao eram chamados de "hackers". Aqueles que realmente entendiam do riscado. Vale lembrar que o computador do filme, para quem assistiu, era um Sinclair ZX-80, os disk-drives eram de 8 polegadas e o modem, provavelmente 1.200 bps. Para ilustrar melhor a historia, nos EUA pode-se conseguir um telefone pagando uma taxa de instalacao que nao chega a 100 dolares. No dia seguinte os caras vem na sua casa e voce ja' pode fazer o que quiser com ele. Pode-se inclusive especificar que o seu numero nao conste na linha telefonica (o que muita gente faz, para evitar Tele-marketing). Adicione a isso, o fato de que com as novas versoes de computador, muita gente vendia o seu micro a preco de banana (mais ou menos como as pessoas estao vendendo hoje os seus XTs).

Muita gente comecou a comprar seus modems e tentar fazer acessos indevidos, sozinhos ou em turmas. Acessar BBSes virou mania, assim como criar BBSes, tanto por farra como para ganhar dinheiro. A pirataria de software, como games e utilitarios era uma forma pratica de economizar. Descobrir como remover a protecao daquele jogo "quentisssimo" era o maximo em desafio.

As pessoas usavam truques para nao pagar altas contas telefonicas, se comunicavam atraves de BBSes e trocavam arquivos de computador com coisas interessantes, por exemplo: como fazer explosivos, como entrar no computador da companhia aerea PAN-AM, como falsificar a carteira de motorista (para poder comprar ou beber cerveja), trocar numeros de cartoes de credito, etc. Pro brasileiro, isso pode parecer incrivel, ja' que vivemos uma ditadura, mas nos EUA, so' cometer um assassinato e' que e' crime: descrever um assassinato nao e'. Duvido muito que a maioria das pessoas que fizessem o download de um arquivo explicando a fabricacao de Napalm realmente fizessem

o dito cujo em casa. Mas a possibilidade de bancar o espiao e mexer com coisas proibidas mexe com a cabeca das pessoas. Livros de James Bond sempre tiveram alguma saida, e o fato de eles descreverem fabricacao de bombas ou como matar alguem com um golpe de mao nunca foi motivo serio para a censura. Para quem acha que nao, existe uma referencia no "Hacker Crackdown" sobre o interesse de Steven Jobs e seu colega de criacao da Apple Inc, com relacao a fabricacao de "Blue Boxes".

Voltando aos acessos ilegais, haviam os que se dedicavam a isso como forma de testar seus conhecimentos de informatica. Conhecia-se muito pouco sobre seguranca de informatica, a informacao a esse respeito era guardada a sete chaves e compartilhada aos 4 ventos,(no "Computer Underground"),ja' que a pessoa que conseguia entrar num sistema grande muitas vezes fazia questao de comentar como havia feito isso:

:back door: (porta dos fundos) n. um buraco na seguranca do sistema
deixado deliberadamente por projetistas ou controladores. A motivacao
de tais buracos nao e' necessariamente sinistra; alguns sistemas
operacionais, por exemplo, sao lancados com contas de acesso privi-
-legiado intencionados para tecnicos de manutencao ou programadores
da equipe de suporte tecnico da empresa.
Syn. {trap door}; pode ser chamado tambem de`wormhole'. Veja tambem
{iron box}, {cracker}, {worm}, {logic bomb}.

Historicamente, as"portas de servico"ou "dos fundos" sempre pintaram
em sistemas (operacionais) por mais tempo do que alguem esperava ou
planejava te-las, e umas poucas ficaram bastante conhecidas.
A infame {RTM} "worm" de 1988, por exemplo, usava uma porta de
servico na ferramenta de "sendmail" do UNIX {BSD}.

A palestra ganhadora do premio Turing de 1983, feita por Ken Thompson
(nota: desenvolvedor do Unix) revelou a existencia de uma porta de
servico nas primeiras versoes do UNIX que talvez possam ter qualifi-
cado como a "haqueada" de seguranca mais traicoera e inteligente
-mente feita de todos os tempos. O compilador C continha codigo que
reconhecia a senha escolhida por Thompson, dando a ele entrada para
o sistema independente do fato de existir ou nao uma conta criada
para ele.

Normalmente, tal "porta dos fundos" poderia ser removida atraves da
edicao do codigo fonte para o compilador e a posterior recompilacao
do compilador. Mas para recompilar o compilador, voce *precisa* usar
o compilador --- de forma que Thompson tambem arrumou para o compila-
dor reconhecer quando estava compilando uma versao de si proprio*, e
inseria no compilador recompilado o codigo para inserir no "login"
recompilado para permitir a entrada de Thompson --- e, claro, o codi-
go para reconhecer a si mesmo e fazer a coisa toda novamente a
proxima vez que isso acontecesse! E tendo feito isso antes, ele era
capaz de recompilar o compilador atraves das fontes originais; essa
"haqueada" se perpetuava invisivelmente, deixando a porta dos fundos
ativa e no lugar, mas com nenhum traco nas fontes.

Esta conversa que revelou o esquema foi publicada como
"Reflections on Trusting Trust", "Communications of the
ACM 27", 8 (August 1984), pp. 761--763.

Nao e' incomum o proprio autor revelar como fez esse tipo de esquema. A motivacao por tras disso era a de que nao se intenciona mal algum com tais acessos ilegais. Se um sistema e' invadido, mas nenhum arquivo foi apagado, nada foi alterado, nem ninguem ficou sabendo, qual seria o crime? Definiu-se nessa epoca a:

:hacker ethic, the: n. 1. A crenca em que a partilha de informacoes e' uma ferramenta poderosa, e que e' um dever etico dos hackers partilhar sua pericia atraves da escrita de software gratis e facilitar o acesso a informacao e a recursos de computacao, sempre que possivel. 2. A crenca que craquear sistemas por diversao e exploracao e eticamente certo, sempre que o craqueador nao cometa roubo, vandalismo ou quebra de confianca.

Ambos estes principios normativos eticos sao mundialmente, mas nao universalmente, aceitos entre hackers. Alguns hackers consideram a etica hacker no primeiro lance, e muitos continuam nele atraves da escrita e distribuicao de software gratuito. Uns poucos vao mais alem e asseguram que *toda* informacao deveria ser gratuita e que *qualquer* direito ou controle de posse e' ruim; esta e' a filosofia por tras do projeto {GNU} (obs: grupo que se dispos a escrever em conjunto, software de qualidade que seria distribuido sem direitos autorais)

O sentido 2 e' mais sujeito a controversia: algumas pessoas consideram o craquear em si algo eticamente tao ruim quanto invasao de domicilio. Mas a crenca de que craqueada "etica" exclui a destruicao pelo menos modera o comportamento de gente que se veria na posicao de "craqueadores benignos" (ver tambem {samurai}). Dentro desta visao, pode ser uma das maiores formas de cortesia (a) invadir um sistema, e entao (b) explicar para o Sysop ou encarregado, de preferencia por E-mail de uma conta {superuser}, exatamente como isso foi feito e como o buraco pode ser fechado --- agindo como um {tiger team} voluntario e gratuito.

A mais autentica manifestacao de ambas as versoes da etica hacker e' que quase todos os hackers estao ativamente interessados em partilhar truques tecnicos, software, e (quando possivel) recursos de computacao com seus colegas. Grandes redes cooperativas tais como: {USENET}, {FidoNet} e Internet (ver {Internet address}) podem funcionar sem controle central por causa deste trato; eles tanto acreditam como reforcam o sentido de comunidade que pode ser o mais valioso bem da Hackermania.

Existem varias razoes para se partilhar sabedoria entre gente que mexe com computadores. E' facil descobrir em meia hora de conversa, que todo mundo pode estar sabendo de um jeito mais facil de se solucionar um problema que uma pessoa sozinha pode demorar dias e dias para descobrir. E haja problemas..

Mesmo hoje, muitos programas e sistemas operacionais sao lancados no mercado contendo defeitos, que sao corrigidos em versoes posteriores. Em algumas ocasioes, sao feitos arquivos contendo os remendos, que sao denominados "patch". Isso acontece porque os programas sao desenvolvidos por conjuntos de pessoas, ou ate' grupos de grupos, trabalhando em diferentes partes do sistema, com varios chefes ou ausencia deles. O trabalho de debugar e testar os prototipos tambem nao e' exatamente glamuroso ou interessante. Caracteristicas novas ou "inovadoras" sao mantidas em segredo. Os programadores, de forma geral, ja' tem um trabalho enorme em fazer o prototipo funcionar, de forma a ser "fool-proof", imagine faze-lo funcionar de forma a ser "smart-proof". O fato do sistema funcionar sem falhas, nao impede de haver algum erro esperando para causar um crash no sistema. Para se ter uma ideia, o codigo fonte de um programa pode atingir milhares ou as vezes milhoes de linhas, no caso de programas complexos, destinados a controlar o sistema telefonico de uma cidade, por exemplo.

No dia 15 de janeiro de 1990, aconteceu um defeito numa estacao

telefonica de Manhattan. O problema e' que ele contagiou outras estacoes, como um virus de computador. Como aconteceu no feriado de Martin Luther King, ficou suspeito como algo provocado por uma pessoa, e nao como um defeito tecnico que desencadeou uma reacao em cadeia. As pessoas tinham medo de que isso pudesse acontecer, e comecaram a procurar provas que fundamentassem suas suspeitas.

Outros "crashes" aconteceram. O mais espetacular foi no dia 17 de setembro de 1991. Algumas estacoes telefonicas ficaram sem energia e pararam de funcionar. Isso cortou as comunicacoes de aeroportos como Kennedy, La Guardia e Newark. Naquele tempo, esse tipo de pesadelo ja' existia, na forma de um filme chamado "Duro de matar" (Die Hard II). Cerca de 500 voos tiveram de ser cancelados. E outro tanto na Europa. 85000 passageiros foram prejudicados e estes nao puderam usar o telefone para avisar suas familias do problema. A AT&T ficou com uma pessima imagem por causa desse episodio, que nao teve nada a ver com "computer abusers".

Mesmo assim, e' sempre mais facil se apelar para um bode expiatorio. Hitler pos a culpa da crise economica da Alemanha nos Judeus, para se promover. Alguns "espertos" pegos em flagrantes eram exemplos de "genialidade" a servico do mal, sendo que os bons exemplos, responsaveis pela construcao da Usenet, por exemplo, eram ignorados.

No inicio, era muito dificil o sujeito ser condenado por esse tipo de coisa. Ate' a mae de um cracker reclamar para um politico sobre isso, artificios, como provar que a conexao do computador do intruso roubava energia, (crime previsto na legislacao) eram recursos validos. Isso gerava publicidade e em alguns casos, nenhuma ou pouca condenacao.

Entao a pessoa envolvida saia no jornal, com o mesmo tipo de fama que os caras que picharam o Cristo Redentor sairam (alguem sabe que um deles foi assassinado em condicoes misteriosas, por falar nisso? Isso e' Brasil). Dava entrevistas, ou era recrutado (no caso de fraude telefonica) para ajudar a cacar colegas que faziam isso. Ate' podia entrar para o ramo da seguranca eletronica (ja' que tinha otimas/pessimas referencias).

A coisa ficou tao seria que o governo e as grandes companhias, como a carinhosamente apelidada de Ma BELL, comecaram a ficar preocupadas. Quando um cara crackeava uma empresa telefonica, por exemplo, e era julgado, a falha era divulgada. Custava muito condenar o mau elemento e pior: a falha ficava exposta ate' que o sistema fosse trocado, coisa que nao acontecia do dia para a noite. Imagine re-treinar o pessoal que usa o sistema, trocar senhas de acesso, numeros de telefone, talvez redesenhar o software invol--vido, e Deus sabe o que. Sem falar na perda de credibilidade da empresa que sofresse o ataque.

Para poupar um pouco a digitacao, aqui vai alguns press-releases:

****
****

PRESS RELEASE

FOR IMMEDIATE RELEASE:
Wednesday, May 9, 1990

CONTACT: Wendy Harnagel
United States Attorney's Office
(602) 379-3011

PHOENIX--Stephen M. McNamee, United States Attorney for the District of Arizona, Robert K. Corbin, Attorney General for the state of Arizona, and Henry R. Potosky, Acting Special Agent in Charge of the United States Secret Service Office in Phoenix, today announced that approximately twenty-seven search warrants were executed on Monday and Tuesday, May 7 and 8, 1990, in various cities across the nation by 150 Secret Service agents along with state and local law enforcement officials. The warrants were

issued as a part of Operation Sundevil, which was a two year investigation into alleged illegal computer hacking activities.

The United States Secret Service, in cooperation with the United States Attorney's Office, and the Attorney General for the State of Arizona, established an operation utilizing sophisticated investigative techniques, targeting computer hackers who were alleged to have trafficked in and abuse stolen credit card numbers, unauthorized long distance dialing codes, and who conduct unauthorized access and damage to computers. While the total amount of losses cannot be calculated at this time, it is

(MORE)

estimated that the losses may run into the millions of dollars. For example, the unauthorized accessing of long distance telephone cards have resulted in uncollectible charges. The same is true of the use of stolen credit card numbers. Individuals are able to utilize the charge accounts to purchase items for which no payment is made.

Federal search warrants were executed in the following cities:

Chicago, IL
Cincinnati, OH
Detroit, MI
Los Angeles, CA
Miami, FL
Newark, NJ
New York, NY
Phoenix, AZ
Pittsburgh, PA
Plano, TX
Richmond, VA
San Diego, CA
San Jose, CA

Unlawful computer hacking imperils the health and welfare of individuals, corporations and government agencies in the United States who rely on computers and telephones to communicate.

Technical and expert assistance was provided to the United States Secret Service by telecommunication companies including Pac Bel, AT&T, Bellcore, Bell South, MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West, and by the many corporate victims. All are to be commended for their efforts in researching intrusions and documenting losses.

Resumindo a historia acima, um monte de mandados foram executados nos EUA com a assistencia tecnica de empresas, tais como a Nynex, Bellcore, AT&T, etc, (todas elas do porte quase de Estatais, que tinham perdas devido a acao de tais individuos) e uns tres individuos ja' haviam sido presos no dia anterior. Esse tipo de acao, envolvendo cerca de 150 agentes do servico secreto, junto com policiais e membros de forcas locais era parte da operacao de dois anos chamada Sundevil.
Os prejuizos alegados, provocados por alguns poucos individuos poderiam estar chegando a casa de milhoes de dolares, decorrentes do trafico ilegal de numeros de cartoes, credito, chamadas telefonicas sem pagar, acesso nao autorizado de computadores.

A ideia, claramente expressa era de mandar uma mensagem a "computer hackers" que teriam violado as leis dos EUA na crenca de que estariam inviseis atraves do uso do computdor.

Tendo como instrumento o "Comprehensive Crime Control Act" que proibe a fraude com cartao de credito e a fraude com computador, o Servico Secreto americano alegava ter feito 9000 prisoes, a partir do momento em que a lei

foi lancada, em 1984.
A explicacao oficial era mais ou menos assim, traduzida:

"Recentemente nos temos testemunhado um alarmante numero de gente jovem que, por uma variedade de razoes de ordem psicologica e sociologica, tem ficado pregados a seus computadores e estao explorando seu potencial de forma criminosa. Frequentemente, a progressao da atividade criminal ocorre quando envolve fraude de telecomunicacoes (ligacoes interurbanas gratuitas), acesso nao-autorizado a outros computadores (seja por dinheiro, fascinacao, ego ou desafio intelectual), fraude de cartao de credito (dinheiro ou compra de bens materiais), e entao se movimentam para outras destrutivas atividades como virus de computador."
"Alguns computer abusers formam associacoes intimas com outras pessoas tendo interesses similares. Grupos underground tem sido formados com o objetivo de trocar informacao relevante as suas atividades criminais. Estes grupos sempre se comunicam entre si atraves de sistemas de mensagens entre computadores denominados BBS "Bulletin Boards".

Quem nao entendia nada do assunto, lia e achava otimo que o governo estivesse fazendo alguma coisa para parar com esse tipo de ameaca. Quem sabe se ele tivesse sucesso, as companhias telefonicas jamais errariam na hora de cobrar a conta, nem os bancos deixariam de "cair o sistema" quando precisamos dele, etc. Esse tipo de coisa deixaria de acontecer. E o comunicado oficial dizia que 27 mandados de busca haviam sido feitos em 12 cidades. Tudo bem, so' que nenhum resultou em prisao. Cerca de 40 computadores e 20.000 discos foram apreendidos, em todo pais, segundo noticias. Em varias noticias, nunca a falta o uso do "would be", "may be" e numeros alarmantes. "As perdas que *estimamos* podem chegar a milhoes de dolares", de acordo com um promotor do Arizona. Nenhuma certeza, opiniao de um sujeito que nao era do ramo de telecomunicacoes. Talvez tenha acontecido aquele tipo de situacao em que o sujeito comete um assalto num banco, que declara entao um prejuizo de dois milhoes. O assaltante, preso, fala que so' roubou um milhao. Ja' a policia, esta alegava so' ter recuperado metade do valor. Qual estaria dizendo a verdade? Nao acho impossivel de acontecer esse tipo de coisa. Mas retornando a Operacao Sundevil...

Mesmo assim, muita gente teve equipamento confiscado. Poucos foram presos por cometerem crimes eletronicos. A operacao fracassou em varios aspectos. Houve acoes arbitrarias, como o confisco de equipamento orcado em 20000 dolares de um no' internet, e o caso do Steve Jackson Games. Neste, o servico secreto americano apreendeu material que seria usado para a confeccao de um jogo, do tipo do WAR ou DIPLOMACY (melhor seria dizer Role-Playing-Game) sob a alegacao de que era material de ensino para Hackers. Este jogo ja' foi traduzido para o portugues, e se chama GURPS CYBERPUNK (o preco do manual esta' em torno de 24 Reais). Nas primeiras paginas do mesmo esta' inclusa uma descricao sumaria da historia toda. No julgamento de Steve Jackson, o Servico Secreto foi mais ou menos taxado de incompetente e condenado a pagar indenizacao pelo prejuizo causado (o jogo teve que ser reconstruido, ja' que muito do material foi destruido durante o confisco).

Quem ler o livro "The Hacker Crackdown" do Bruce Sterling, ira' ter um retrato maior da historia toda. Uma parte interessante, porem, e' o fato de que muita pouca gente que fez o "raid" contra os "hackers" sabia o suficiente de computacao para isso. Entao acontecia do "especialista" de plantao mandar um policial fazer uma copia de um disquete apreendido e o cara colocava o dito na maquina de XEROX. Da mesma forma, essa carencia de gente que entende alguma coisa de modus operandi deve ter feito a tristeza de muitas pessoas e ate' adolescentes, que foram confundidos com "computer abusers". Imagine a cena abaixo:

"Um "blitz" de hacker tipica e' mais ou menos desse jeito. Primeiro,

a policia entra rapidamente, atraves de todas as aberturas, com forca superior, na presumcao que esta tatica ira' diminuir as baixas ao minimo. Segundo, possiveis suspeitos sao imediatamente removidos da vizinhanca de todo e qualquer computador, de forma que eles nao terao chance de queimar ou destruir evidencia. Suspeitos sao amontoados numa sala sem computadores, e mantidos sob guarda - *desarmada*, ja' que as armas sao sutilmente guardadas, mas a mostra, de qualquer forma. Eles recebem o mandado de busca e sao avisados de que qualquer coisa que disserem podera' ser usada contra eles. Normalmente eles tem muito o que dizer, especialmente se sao pais sem nenhuma suspeita".
(Bruce Sterling - The Hacker Crackdown)

E', algumas pessoas ficaram chocadas, ja' que a policia americana tem um certo respeito pela lei e nao fazem blitz desse genero contra casas de traficantes de drogas, por exemplo. E se o Press Release mostrado acima estivesse correto, usar uma forca policial de certa magnitude, invadindo sua casa para levar seu irmao ou filho de talvez 16 anos, e' algo parecido a usar canhoes para matar moscas. A ideia era, de um lado, usar justificativas para esse abuso de autoridade, digno do livro "1984", de George Orwell (por sinal, muito comentado entre os hackers, principalmente nos EUA, onde e' leitura obrigatoria no 2o Grau).

Para facilitar a acao desse tipo de coisa, explorou-se muito os "crimes perfeitos". Logo, ja' que ninguem sabe exatamente o que e' um hacker, o que ele faz de bom ou de ruim, e muito menos gente entende o que e' um computador, porque nao transformar esses adolescentes em prototipos de super-criminosos? Foi o que aconteceu com muita gente. A comunidade eletronica chegou ate' a tentar a divulgacao de outros termos, como o de "cracker", para evitar o mal-uso da palavra "hacker".

:cracker: n. Alguem que quebra a seguranca de um computador. orig. 1985 usada por hackers contra o mau-uso jornalistico da palavra {hacker} (q.v., sense 8). Uma tentativa anterior de se usar`worm' neste sentido por volta de 1981--82 na USENET foi largamente um fracasso.

O uso de ambos neologismos reflete uma forte revolta contra o roubo e o vandalismo perpetrados por grupos de craqueadores. Enquanto e' esperado que qualquer hacker real tera' feito algum craqueamento inteligente e conhece tecnicas basicas, alguem pos {larval stage} supostamente deveria ter ultrapassado o desejo de faze-lo, exceto por razoes praticas de fim imediato (por exemplo, se e' necessario circundar alguma medida de seguranca para se conseguir fazer um determinado trabalho).

Embora "craqueadores (crackers)" sempre gostam de se descrever a *si proprios* como hackers, a maioria dos verdadeiros hackers consideram-os como uma forma de vida separada e mais baixa.

Consideracoes eticas aparte, hackers consideram que qualquer um que nao pode imaginar uma forma mais interessante de brincar com seus computadores que invadir o de outra pessoa, tem que ser bem {losing}.(ver o Jargao)

:cracking: n. O ato de "invadir" um computador; aquilo que um {cracker} faz. O contrario do que se possa pensar, isso normal mente nao involve um brilhantismo, mas persistencia e repeticao de um punhado de truques bem-conhecidos que exploram fraquezas na seguranca de sistemas-alvo. A maioria dos crackers sao hackers mediocres.

:dark-side hacker: n. Um hacker criminoso ou malicioso; um
   {cracker}. Do personagem Darth Vader (Guerra nas Estrelas),
   "seduzido pelo lado escuro da forca". A implicacao de que
   os hackers formam uma especie de cavaleiros Jedi de elite
   e' intencional.

Isso nao funcionou. O "hacker" virou sinonimo de bandido eletronico. O fato de que muitos adolescentes eram pegos fazendo isso ate' criou o mito de que a idade media do "hacker" varia entre 15 e 18 anos, quando na verdade, os realmente inteligentes dificilmente se conhece a existencia.

Nao existe muito glamour nos verdadeiros bandidos e vandalos eletronicos. No livro "Seguranca de Computador" (um do mesmo autor de "Computer Crime". Infelizmente me roubaram o livro ha' alguns anos) dentre varios casos listados, estava o de um faxineiro que se divertia em quebrar circuitos eletronicos de um mainframe da empresa onde trabalhava."So' para ver aquela maquina imensa parar de trabalhar".

Atualmente, se fizermos uma analogia, quem pensa em se instruir mais sobre o assunto enfrenta o mesmo tipo de preconceito que as pessoas que se interessavam por artes marciais enfrentavam ha' algum tempo atras. So' apos series de televisao, como "Kung-fu", comecou-se a pensar que praticantes de Karate e Capoeira nao sao assassinos em potencial. Na minha infancia, falava-se de capoeiristas como se fala do diabo. Pra explicar que o aprendizado de uma arte cria (parte das vezes) uma mentalidade que o praticante nao se sente motivado a abusar do que sabe, isso e' algo que demora a entrar na cabeca das pessoas.

O verdadeiro interessado em cometer crimes informaticos nunca ira' fazer propaganda disso. Nem ira' usar sua propria conta ou acesso a uma maquina para cometer suas barbaridades. Seria como um pichador fazer suas "obras" dentro dos muros de sua casa. E aqueles interessados em roubar bancos, bom.. existe muito mais informacao hoje sobre isso do que antes. Aquele que se interessou ontem por seguranca informatica, amanha estara' desenvolvendo sistemas mais seguros. Foi um "hacker" que auxiliou na captura de Mitnick. Este especialista nao foi criado lendo manuais de "boa norma e conduta" no uso de computadores.

Mas as pessoas que administram os computadores, o publico de forma geral, este dificilmente se interessa em acender a luz e apagar o mito. Quem sabe com o caso Mitnick, as pessoas se interessem em descobrir que existe gente bem intencionada, que sabe muito sobre computadores e que nao esta' interessada em assaltar bancos ou atrapalhar a vida das pessoas. Quem sabe? A soma da inteligencia na terra parece ser uma constante, mas a populacao esta' crescendo (Lei de Murphy).

:samurai: n. Um hacker de aluguel para craquear legalmente sistemas,
   peruando faccoes em lutas corporativas politicas, advogados
   perseguindo leis de privacidade e casos da primeira emenda
   e outras partes com razoes legitimas para precisar de um
   "abre-portas" eletronico. Em 1991, a midia reportou a existencia
   de uma cultura de samurai que se encontra eletronicamente em
   BBSes, a maioria deles de adolescentes com PC; eles modelaram
   eles mesmos explicitamente no samurai historico do Japao e nos
   "net cowboys" das novelas de William Gibson's {cyberpunk} .
   Aqueles entrevistados clamam aderir a um rigido codigo de leal
   -dade aos seus empregadores e desdem por vandalismo e roubo
   praticados por hackers criminosos contrarios a etica hacker;
   Alguns se referem ao livro de Miyamoto Musahi "O livro dos cinco
   aneis", um classico da doutrina samurai.
   Ver tambem {Stupids}, {social engineering}, {cracker},
   {hacker ethic, the}, e {dark-side hacker}.

No filme "SNEAKERS" existe essa preocupacao, de mostrar que e' util ter um

sujeito que realmente entenda desse assunto. Nao se consegue impedir o crime eletronico "castrando" o intelecto de quem se interessa por ele. Uma propaganda que vi na revista (extinta) Hack-Tic coloca isso:

"Sabotage is as simple as pulling a plug".

Fica aqui a sugestao a aqueles que se interessam pelo assunto, que tomem muito, mas muito cuidado com a lingua. Em muitos empregos, nao se precisa de um genio, mas de gente cuja idoneidade nao seja posta em duvida. Isso significa nao deixar arquivos com nomes "compcrime.doc" no seu espaco de disco. Se tiver de discutir alguma falha de seguranca no sistema, pense bem: sera' que um colega de trabalho nao te acusara' de utilizar aquela falha? Ou pior, sera' que ele nao a utiliza? Repito: pense duas vezes ou mais, antes de conversar sobre seguranca de computadores. Pense mais vezes antes de experimentar qualquer coisa anormal no seu local de trabalho.
E respeite aquilo que te mandarem respeitar. A confianca e' algo que, uma vez perdido, dificilmente e' recuperado.

NEWS - SECCAO DE CARTAS

CARTAS DE APOIO

Dentre as varias cartas elogiando o jornal, recebi esta, publicada com com permissao da figura. Pode ser util, no futuro:

Olah Derneval,

Gostei muito do BARATA ELETRICA, se bem que que acho que voce poderia colocar um nome mais condizente e fica ai a sujestao. Bom, sou SysOp da InfoNet BBS, Brasilia/DF e caso voce decida a colocar mais edicoes, tem todo o meu apoio e inclusive criarei uma area de arquivos soh para o danado.

Outro ponto de vista que tenho e que achei ele muito longo e minha outra sujestao que voce entitule o mesmo como um boletim.

Ah, caso queira fazer uma visita qualquer dia desse e so ligar:

Sistema.....: InfoNet BBS
SysOp.....: Regivaldo Costa
Fone.....: (061) 351-8604
Horario.....: 24 horas no ar!!!
Configuracao.....: De 1200 a 14.400 bps (Emulacao ANSI)

Abracos,

Regivaldo Costa

Resposta: No futuro eu explico minha insistencia com um nome desses. Quanto ao tamanho...e' muita coisa. Eu nao sei se amanha vou poder escrever de novo. Melhor muito do que pouco (acho).

Caros colegas...

esse e' o meu primeiro mail para todos voces, e espero que seja bem recebido. Primeiramente, gostaria de parabenizar o Derneval pela sua iniciativa de criar essa lista de discussao. Espero que todos possam contribuir tanto quanto extrair informacoes uteis que serao compartilhadas entre todos. O espirito que essa lista deve ter e' o de hacker, porem nao no sentido "negro" da palavra. Se voces estao na lista do Derneval, e' porque certamente voces devem ser aficcionados por computacao (no minimo).

Antes de escrever mais e mais, deixe-me apresentar-me... Eu sou Mauricio Walder, tambem conhecido por Darth Walder ou Lord Morpheus (no talker Dreaming). Espero que isso nao crie confusoes, pois ja' vi que temos um Morpheus na nossa lista... Creio que o uso de "nicknames" ou "handles" e' muito comum, e muito interessante. Bom, continuando... Eu estou atualmente no terceiro ano de Engenharia Agronomica na ESALQ/USP (Escola Superior de Agricultura 'Luiz de Queiroz') em Piracicaba, SP. Sim, eu sei que Eng. Agronomica nao tem muito a haver com computacao, mas eu sempre gostei. Mexo com computadores desde 1984, quando morei 1 ano nos USA. Em 1989 comecei a trabalhar no CIAGRI (Centro de Informatica na Agricultura) aqui na ESALQ. Atualmente estou fazendo estagio no CENA (Centro de Energia Nuclear na Agricultura) trabalhando com computacao (logico) aplicado `a agricultura. Por causa disso, tenho acesso direto `a Rede, e trabalho com Unix e Windows NT. Tenho varias contas Internet, porem prefiro usar a (mwalder@carpa.ciagri.usp.br) para correspondencia, ou a mwalder@pintado.ciagri.usp.br).

Eu morei 2 anos nos USA em 1990, e la' entrei em contato com os BBSs da vida. Curti pra burro. Eu acessava alguns BBSs meio "underground" - nada de programas piratas, apenas alguns textos meio subversivos e outras coisas do tipo. Portanto desde aquela epoca eu ja' conhecia aquele texto "A Night of Hackers" que o Derneval enviou a pouco para todos. Uma coisa que me estimulou muito na epoca foi que la' eu nao tinha q.arcar com um gasto absurdo em ligacoes de telefone (como todos tem aqui). Podia utilizar a maioria dos BBSs sem pagar nada por muito tempo (logicamente com um certo tempo e quantidade de download limitada).

Em 1992 eu regressei a Piracicaba, e fiquei sem mexer em nada de BBS, pois nao havia nenhum. Agora existem 4, mas nenhum muito bom... Infelizmente nao posso acessar os de Sao Paulo, pois os custos de uma ligacao DDD sao exagerados... Como nao quero gastar dinheiro com uma coisa que nao e' muito quando comparado `a Internet (a qual eu tenho acesso de graca aqui) comecei a me dedicar pra valer `a Internet. Eu ja' tinha utilizado a BITNET e a USENET, mas a Internet me mostrou ser muito maior, e muito mais poderosa, com muitos recursos exploraveis. Portanto, apesar de ser bem geralista, meu norte e' a Internet.

Eu curto pra caramba aprender sobre novos locais, e utilizar novas ferramentas e tenho utilizado ftp, telnet, gopher, www, lynx, mosaic, netscape, netfind, archie, wais, veronica, whois, irc, bla bla bla... Com certeza alguns de voces nao tem a menor ideia do seja tudo isso - e nem precisa. No futuro faco um texto pra explicar isso melhor.

Me dedico atualmente a preparar uma apostila para os usuarios da Internet daqui (Campus da USP de Piracicaba). O CIAGRI colocou um computador `a disposicao dos professores e alunos, mas nao existe nenhum material de introducao para os recursos mais elementares de pesquisa que a rede oferece. Nisso, a maioria dos usuarios abre conta so' para enviar/receber mail e utilizar o IRC apenas (o que eu acho ridiculo, pois existe MUITO mais coisa interessante para se fazer na Internet - principalmente na area academica e cientifica, mas tambem na parte de entretenimento), e o CIAGRI ganha uma grana preta ministrando cursinhos bem ruins sobre a utilizacao da Internet. Com a apostila, passo meu conhecimento adiante, preencho a lacuna e diminuo meu trabalho. Nao aguento mais fazer isso sozinho.

Bom, agora sobre as minhas opinioes sobre essa lista. Eu recebi a mensagem do nosso colega Izar la' de Israel, que estava descontente com o

movimento da lista. Eu gostaria de pensar que o movimento esta' baixo por que a maioria do pessoal e' estudante, e como tal, ainda esta' de ferias aqui no Brasil... Espero que o movimento aumente com o passar do tempo. Porem se todos forem desistindo, nunca havera' uma lista que tenha continuidade. Portanto, vamos fazer uma forcinha. Outra coisa: o Derneval teve o trabalho de criar uma lista especifica no servidor da UNICAMP, e porem, como eu acabei de ver numa mensagem, apenas 16 pessoas se cadastraram.(obs: atualmente o numero ultrapassou a marca de 50 inscritos).

Eu gostaria de pedir a todos voces que enviassem uma pequena mensagem para todos os outros membros da lista, se apresentando, para que nos possamos nos conhecer melhor. Acho que esse seria um primeiro passo na direcao certa.

Eu tenho um outro assunto a propor para todos, mas irei faze-lo em uma outra mensagem, para nao complicar muito...

Aguardando mensagens de todos voces,

envio os meus abracos...

-=-

=========
TALKER II
=========

Buenas...

A sugestao que eu gostaria de fazer e' a utilizacao de um talker para uma discussao on-line (semelhante ao IRC porem mais proximo e portanto bem mais rapido). Eu ja'tenho um talker rodando, e ja' tendo passado por uma fase de teste de varios meses, ja' esta' funcionando direito (fora algumas travadas que ocorrem quando o sistema aqui esta' sobrecarregado ou a conexao remota da' problemas). `As vezes ele sai do ar, mas sempre tem eu e o Floyd monitorando, e nos estamos regularmente dando "boot" nele. O talker por enquanto esta' com o nome de "Realms of Dreaming" - em homenagem ao reino do Lord Morpheus (quem le "Sandman" do Neil Gaiman manja). Ja' temos varios usuarios cadastrados la' (mais de 120), mas nao temos muito trafego, pois comecamos apenas com alguns amigos, depois amigos dos amigos, e por ai' foi. A maioria dos usuarios logou-se apenas uma vez, e como estava vazio, nao conversou com ninguem, nao gostou e depois nunca mais voltou. O Dreaming esta' aberto a qualquer um - voce pode entrar e colocar o seu "handle". Se ninguem ainda o tiver registrado como seu, basta colocar' a sua senha e pronto. Foi um trabalho enorme. Organizar tudo organizando tudo, colocando todos os helps, enfim, tentando torna'-lo o mais amigavel possivel. Ah! Somente aqueles usuarios com acesso direto `a Internet poderao acessa'-lo... Para dar uma olhada no Dreaming, deem "telnet carpa.ciagri.usp.br 3000".

Eu peco encarecidamente que todos os usuarios leiam todas as mensagens que aparecem la' - nao sao meros enfeites, e que leiam os helps antes de sairem perguntando tudo. Outro pedido (que esta' escrito la') e' que todos os novos usuarios que desejem se cadastrar para utilizar regularmente o sistema enviem um mail para mim, com o seu endereco de E-mail e o username que foi registrado no Dreaming. Essa informacao e' apenas para o meu conhecimento, nenhum outro usuario do Dreaming tera' acesso a essa informacao.

Para que voces conhecam um pouco mais sobre o talker, eixe-me citar alguns recursos existentes la':

- voce pode listar todos os comandos atraves do .help (ou .h)
- todos os comandos sao precedidos por um ponto (.)
- voce pode escrever mensagens publicas no board de cada sala
- voce pode enviar e receber mensagens pessoais para outros

usuarios (como um sistema de E-mail)
- voce pode entrar numa sala com outra pessoa e "tranca'-la",
tornando-a "particular" ou "privada", como quiserem. Outras pessoas so'
poderao entrar nessa sala se alguem de dentro convidar
- voce pode conversar particularmente com uma outra pessoa sem
que as outras pessoas na sala vejam ("whisper")
- voce pode listar todas as pessoas utilizando o talker
- voce pode GRITAR para que todas as pessoas em todas as salas
vejam o que voce gritou
- e muitas outras coisas...

Devido `a natureza "sensivel" de algumas informacoes que nos compartilhamos, me foi sugerido que eu criasse um outro talker, separado do talker - para que outros usuarios, que nao tem nada a haver com o nosso assunto, ficassem olhando. E' possivel construir um outro talker, em uma outra porta, que tivesse acesso restrito. Um outro recurso de seguranca poderia ser que esse talker nao teria registro de novos usuarios livres - ou seja, todos os usuarios teriam que ser registrados por mim, e qualquer novo usuario deveria pedir permissao especifica via mail para mim - e essa permissao seria discutida pelo grupo, ou se for indicado diretamente por algum membro. E' uma simples questao de todos darem uma olhada no talker e fazerem sugestoes... Eu estou aberto a qualquer sugestao ;-)
Abracos para todos,

|)arth \/\/alder

+---+----------------+
| Mauricio F. A. Walder - mwalder@pintado.ciagri.usp.br | * USP * |
| CIAGRI - Centro de Informatica na Agricultura +----------------+
| ESALQ - Escola Superior de Agricultura Luiz de Queiroz | UNIVERSIDADE |
| Piracicaba - S.P. - BRASIL | de SAO PAULO |
+---+----------------+

| Warning: Don't drink and drive on the `Information Superhighway'!!! |
+---+
"All things are divided into the twin forces of order and chaos, forever
contending for dominance. Life is something that occurs in the interface,
not in the writhing discord of utter chaos, nor in the flatline perfection
of pure order, but somewhere in between." - Dr. Fate in 'Books of Magic'

****

WORM

Esta carta e' meio velha, fala sobre uma worm (programa virus de computador grande porte). Estou colocando aqui so' por causa da opiniao do cara, que eu achei muito engracada. Esta carta e' anterior ao virus "Good Times". Nunca ouvi mais falar do dito.

---------- Forwarded message ----------
Date: Mon, 12 Dec 1994 10:44:00 BDB
From:??????%FAPQ.FAPESP.BR@lion.cce.usp.br
To: Multiple recipients of list RNPTEC-L
Subject: URGENTE! *** WARNING *** - destructive bitnet worm received from BRUFMS

Que sucede, agora os brasileiros estao pegando a moda de gerar viruses?

Sou absolutamente contra a pena de morte. Amputar os cinco membros e' suficiente...

```
|
|
|Date: Sat, 10 Dec 94 00:54:27 EST
|From: ????? ??????
|Subject: *** WARNING *** - destructive bitnet worm received from BRUFMS
|To: ?????@brnlcc, ?????@brufms.BITNET, ????@brlncc.BITNET,
| ?????@fpsp.fapesp.br
|
|Due to the urgency, I am mailing to everybody listed in the BITEARN NODES
|entry for BRUFMS.  I just received a destructive bitnet worm called
|'EMPIRE EXEC'.  This exec sends a copy of itself to everybody in the
|user's NAMES file, and then purges the user's RDR, and then erases
|all * EXEC, * NOTEBOOK, and * NAMES files on the user's 191.  You may wish
|to search your system and delete all copies that you can find, and try to
|track down where/how it started (it may have been created at BRUFMS, or
|received from offsite.  It appears that the comments in the Rexx code are
|in Portugese, so I suspect a Brazilian origin.
|The first 30 lines of the file are:
|/*  EMPIRE CONQUEST FOR CMS - VER1.05 - BY SCARFACE SOFTWARE(1994) */
|'VMFCLEAR'
|'ID (STACK'
|parse pull . . locnod
|SAY;SAY
|hi='1dc8'x;lo='1dc1'x
|SAY'////////////////////////////////////////////////////////////'
|SAY'//        EMPIRE  CONQUEST  FOR CMS   -  VER1.05           //'
|SAY'//                                                         //'
|SAY'//   * SHAREWARE *                   BY SCARFACE SOFTWARE  //'
|SAY'////////////////////////////////////////////////////////////'
|SAY;SAY;SAY
|SAY'INSTRUCOES:'
|SAY;SAY
|SAY'       OBSERVANDO AS POUCAS OPCOES DE GAMES PARA CMS, A SCARFACE'
|SAY'SOFTWARE INOVA TRAZENDO PARA O DOMINIO PUBLICO A VERSAO PARA CMS'
|SAY'DO CLASSICO JOGO EMPIRE CONQUEST. BASICAMENTE PROCURAMOS NAO MO-'
|SAY'DIFICAR A ESSENCIA DO JOGO, ONDE  A  ESTRATEGIA  SEMPRE  SERA  A'
|SAY'A MELHOR DEFESA E OU O MELHOR ATAQUE.'
|SAY'       A VERDADEIRA DIFERENCA ENTRE A VERSOES (DOS/CMS) SERA BA-'
|SAY'SICAMENTE GRAFICA TENDO EM VISTA A IMPOSSIBILIDADE DOS  RECURSOS'
|SAY'GRAFICOS DO CMS. OS OBJETIVOS SAO SIMPLES COMO NA VERSAO P/ DOS,'
|SAY'DOIS PAISES LUTANDO ESTRATEGICAMENTE ENTRE SI A FIM DE  CONQUIS-'
|SAY'TAR O TERRITORIO INIMIGO CAPTURANDO E SUBSTITUINDO SUA BANDEIRA.'
|SAY'       A TELA BASICA DO JOGO ASSEMELHA-SE COM  UM  TABULEIRO  DE'
|SAY'XADREZ ONDE OS MOVIMENTOS DE CADA PECA DE SEU EXERCITO  SE  DARA'
|SAY'ATRAVES DE COORDENADAS ESPECIFICADAS ANTERIORMENTE PELO JOGADOR.'
|SAY'COORDENADAS DIGITADAS ERRADAS PODERAO SER CORRIGIDAS  ESCOLHENDO'
|SAY'A OPCAO RETURN. CADA PECA DE SEU EXERCITO POSSUE UMA  QUANTIDADE'
|SAY'LIMITADA DE HP (FORCA E ATAQUE) SENDO QUE PARA RESTAURA-LAS SERA'
|
|The copy I received came from user CACOM17.  I cannot tell if this
|user is the author, or merely a victim.
|
|                                  Valdis Kletnieks
|                                  Computer Systems Engineer
|                                  Virginia Polytechnic Institute
```

****

********** REUNIAO:

Outra coisa e' a proxima reuniao de (would-be) Hackers aqui na USP (espero). Esta' havendo um clima meio tenso aqui com relacao a lista de hackers que estou fazendo, por isso tenho um ou duas duvidas se vou conseguir a sala. Outra duvida e' o quorum. Na reuniao anterior nao houve nem cinco pessoas. Epoca de prova, sabado de sol, essas coisas. Eu estou querendo marcar outra reuniao, possivelmente talvez ate' chamando a imprensa. Para isso, gostaria que as pessoas que tiverem uma ideia de melhor dia (o mais facil delas aparecerem) que escrevam para a esquina das listas para discutir o lance.

Quem ainda nao sabe acessar a esquina, vai uma dica:

Mande um mail para esquina-das-listas@dcc.unicamp.br

Como texto, coloque:

inscreva hackers (seuemail@sua.maquina) <- sem os parenteses

Assim voce faz parte de uma lista que de vez em quando tem uma pa' de textos interessantes e discussoes sobre o assunto, que envolve ate' seguranca de computadores.
Se voce tiver afim de contribuir, escreva, antes de qualquer texto

submeta hackers

Dessa forma, o listserv entende que voce quer enviar um texto para mais de cinquenta pessoas que atualmente assinam esta lista.

Existe uma possibilidade de se fazer uma reuniao de maniacos de microcomputador. Se voce estiver interessado em participar, mande um mail com o subject:

subject: To^ afim

No corpo da carta podem colocar os dias. Melhor depois da semana santa.

Detalhe: esse "to afim" indica uma presenca certa no local. Gente, se ninguem vier, nunca vai ter uma conferencia de hackers aqui no Brasil. Se poucos responderem, vou marcar um encontro num boteco, com os poucos interessados e alguns que eu ja' conheco. Ah, sim. Para quem nao sabe, isso seria aqui em Sao Paulo. Se nao for possivel, nao fique preocupado. E' uma ideia, nada esta' definido.

A PRISAO DE MITNICK

Muito se escreveu sobre isso. Eu peguei esses arquivos gracas a um anonimo que enviou para a lista. Junto, haviam algumas observacoes, que nao anotei. Basicamente era sobre o exagero em que transformam cada cracker preso.
Se o cara foi preso, tudo bem. Mas muita gente aumenta o tamanho dele para justificar coisas que se fazem para vigiar outros, que nao tem nada a ver com a historia. Do meu ponto de vista, alem de mau-elemento, Mitnick e' um pouco menos do que se fala acerca dele. Dos crimes que se atribuiram

a ele, por exemplo:

From: emmanuel@well.sf.ca.us (Emmanuel Goldstein)
Newsgroups: netcom.general,comp.org.eff.talk,alt.2600
Subject: Re: Mitnick Incident
Date: Fri Feb 17 11:29:43 1995

cmd@aimnet.com (Lord Soth) writes:
>Don't
>you guys think that security is more important than convenience? Stealing
>cc #'s is not all that hard, but you guys seem to make it easier than it
>should be.

The fact of the matter is that they obviously don't. Check out page 34
of the autumn 94 issue of 2600 - "Recent reports indicate that Netcom's
credit file, stored online and containing information on all their
customers, has been compromised." This is old news. It's got nothing
to do with Mitnick; that file has been wide open since August and
Netcom hasn't done a thing about it, despite the warnings. That's
the story no reporter seems to want to write.

emmanuel@well.sf.ca.us

Portanto lembrem-se: pouca gente na imprensa conhece o bastante do
assunto para saber o que esta' falando. Para quem nao sabe, o
autor da carta acima e' o editor-chefe da revista 2600 - Hacker
Quaterly.
Abaixo, outros artigos conseguidos no http://underground.net

Subject: nytimes-021595.html

HOW A COMPUTER SLEUTH
TRACED A DIGITAL TRAIL
NY TIMES, FEB 15 1995

New York Times

RALEIGH, N.C. (8.59 p.m.) -- It takes a computer hacker to catch one.

And if, as federal authorities contend, 31-year-old computer outlaw
Kevin D. Mitnick is the person behind a recent spree of break-ins to
dozens of corporate, university and personal computers on the global
Internet, his biggest mistake was raising the interest and ire of
Tsutomu Shimomura.

Shimomura, who is 30, is a computational physicist with a reputation
as a brilliant cyber-sleuth in the tightly knit community of
programmers and engineers who defend the country's computer networks.

And it was Shimomura who raised the alarm in the Internet world after someone used sophisticated hacking techniques on Christmas Day to remotely break into the computers he keeps in his beach cottage near San Diego and steal thousands of his data files.

Almost from the moment Shimomura discovered the intrusion, he made it his business to use his own considerable hacking skills to aid the FBI's inquiry into the crime spree.

He set up stealth monitoring posts, and each night over the last few weeks, Shimomura used software of his own devising to track the intruder, who was prowling around the Internet. The activity usually began around mid-afternoon, Eastern time, broke off in the early evening, then resumed shortly after midnight and continued through dawn.

Shimomura's monitoring efforts enabled investigators to watch as the intruder commandeered telephone company switching centers, stole computer files from Motorola, Apple Computer and other companies, and copied 20,000 credit-card account numbers from a commercial computer network used by some of the computer world's wealthiest and technically savviest people.

And it was Shimomura who concluded last Saturday that the intruder was probably Mitnick, whose whereabouts had been unknown since November 1992, and that he was operating from a cellular telephone network in Raleigh, N.C.

Sunday morning, Shimomura took a flight from San Jose to Raleigh-Durham International Airport. By 3 a.m. Monday, he had helped local telephone company technicians and federal investigators use cellular-frequency scanners to pinpoint Mitnick's location: a 12-unit apartment building in the northwest Raleigh suburb of Duraleigh Hills.

Over the next 48 hours, as the FBI sent in a surveillance team from Quantico, Va., obtained warrants and prepared for an arrest, cellular telephone technicians from Sprint Corp. monitored the electronic activities of the man they believed to be Mitnick.

The story of the investigation, particularly, Shimomura's role, is a tale of digital detective work in the ethereal world known as cyberspace.

A COMPUTER SLEUTH BECOMES A VICTIM

On Christmas Day, Tsutomu Shimomura was in San Francisco, preparing to make the four-hour drive to the Sierra Nevadas, where he spends most of each winter as a volunteer on the cross-country ski patrol near Lake Tahoe.

But the next day, before he could leave for the mountains, he received an alarming telephone call from his colleagues at the San Diego Supercomputer Center, the federally funded research center that employs him. Someone had broken into his home computer, which was connected to the center's computer network.

Shimomura returned to his beach cottage near San Diego, in Solana Beach, Calif., where he found that hundreds of software programs and files had been taken electronically from his powerful work station. This was no random ransacking: the information would be useful to anyone interested in breaching the security of computer networks or cellular phone systems.

Taunting messages for Shimomura were also left in a computer-altered voice on the Supercomputer Center's voice-mail system.

Almost immediately, Shimomura made two decisions. He was going to track down the intruders. And Lake Tahoe would have to wait awhile this year.

The Christmas attack exploited a flaw in the Internet's design by fooling a target computer into believing that a message was coming from a trusted source.

By masquerading as a familiar computer, an attacker can gain access to protected computer resources and seize control of an otherwise well-defended system. In this case, the attack had been started from a commandeered computer at Loyola University of Chicago.

Though the vandal was deft enough to gain control of Shimomura's computers, he, she or they had made a clumsy error. One of Shimomura's machines routinely mailed a copy of several record-keeping files to a safe computer elsewhere on the network -- a fact that the intruder did not notice.

That led to an automatic warning to employees of the San Diego Supercomputer Center that an attack was under way. This allowed the center's staff to throw the burglar off the system, and it later allowed Shimomura to reconstruct the attack.

In computer-security circles, Shimomura is a respected voice. Over the years, software security tools that he has designed have made him a valuable consultant not only to corporations, but also to the FBI, the Air Force and the National Security Agency.

WATCHING AN ATTACK FROM A BACK ROOM

The first significant break in the case came on Jan. 28, after Bruce Koball, a computer programmer in Berkeley, Calif., read a newspaper account detailing the attack on Shimomura's computer.

The day before, Koball had received a puzzling message from the managers of a commercial on-line service called the Well, in Sausalito. Koball is an organizer for a public-policy group called Computers, Freedom and Privacy, and the Well officials told him that the group's directory of network files was taking up millions of bytes of storage space, far more than the group was authorized to use.

That struck him as odd, because the group had made only minimal use of the Well. But as he checked the group's directory on the Well, he quickly realized that someone had broken in and filled it with

Shimomuru's stolen files.

Well officials eventually called in Shimomura, who recruited a colleague from the Supercomputer Center, Andrew Gross, and an independent computer consultant, Julia Menapace.

Hidden in a back room at the Well's headquarters in an office building near the Sausalito waterfront, the three experts set up a temporary headquarters, attaching three laptop computers to the Well's internal computer network.

Once Shimomura had established his monitoring system, the team had an immediate advantage: it could watch the intruder unnoticed.

Though the identity of the attacker or attackers was unknown, within days a profile emerged that seemed increasingly to fit a well-known computer outlaw: Kevin D. Mitnick, who had been convicted in 1989 of stealing software from Digital Equipment Corp.

Among the programs found at the Well and at stashes elsewhere on the Internet was the software that controls the operations of cellular telephones made by Motorola, NEC, Nokia, Novatel, Oki, Qualcomm and other manufacturers. That would be consistent with the kind of information of interest to Mitnick, who had first made his reputation by hacking into telephone networks.

And the burglar operated with Mitnick's trademark derring-do. One night, as the investigators watched electronically, the intruder broke into the computer designed to protect Motorola Corp.'s internal network from outside attack.

But one brazen act helped investigators. Shimomura's team, aided by Mark Seiden, an expert in computer fire walls, discovered that someone had obtained a copy of the credit-card numbers for 20,000 members of Netcom Communications Inc., a service based in San Jose that provides Internet access.

To get a closer look, the team moved its operation last Thursday to Netcom's network operation center in San Jose.

Netcom's center proved to be a much better vantage point for watching the intruder. To let its customers connect their computer modems to its network with only a local telephone call, Netcom provides dozens of computer dial-in lines in cities across the country.

Hacking into the long-distance network, the intruder was connecting a computer to various dial-in sites to elude detection. Still, every time the intruder would connect to the Netcom system, Shimomura was able to capture the computer keystrokes.

Late last week, FBI surveillance agents in Los Angeles were almost certain that the intruder was operating somewhere in Colorado. Yet calls were also coming into the system from Minneapolis and Raleigh.

The big break came late last Saturday night in San Jose, as Shimomura and Gross, red-eyed from a 36-hour monitoring session, were eating pizza. Subpoenas issued by Kent Walker, the U.S. assistant attorney general in San Francisco, had begun to yield results from telephone company calling records.

And now came data from Walker showing that telephone calls had been placed to Netcom's dial-in phone bank in Raleigh through a cellular telephone modem.

The calls were moving through a local switching office operated by GTE Corp. But GTE's records showed that the calls had looped through a nearby cellular phone switch operated by Sprint.

Because of someone's clever manipulation of the network software, the GTE switch thought that the call had come from the Sprint switch, and the Sprint switch thought that the call had come from GTE. Neither company had a record identifying the cellular phone.

When Shimomura called the number in Raleigh, he could hear it looping around endlessly with a "clunk, clunk" sound. He called a Sprint technician in Raleigh and spent five hours comparing Sprint's calling records with the Netcom log-ins. It was nearly dawn in San Jose when they determined that the cellular phone calls were being placed from near the Raleigh-Durham International Airport.

By 1 a.m. Monday, Shimomura was riding around Raleigh with a second Sprint technician, who drove his own car so as not to attract attention. From the passenger seat, Shimomura held a cellular-frequency direction-finding antenna and watched a signal-strength meter display its readings on a laptop computer screen. Within 30 minutes the two had narrowed the site to the Players Court apartment complex in Duraleigh Hills, three miles from the airport.

At that point, it was time for law-enforcement officials to take over. At 10 p.m. Monday, an FBI surveillance team arrived from Quantico, Va.

In order to obtain a search warrant it was necessary to determine a precise apartment address. And although Shimomura had found the apartment complex, pinning down the apartment was difficult because the cellular signals were creating a radio echo from an adjacent building. The FBI team set off with its own gear, driven by the Sprint technician, who this time was using his family van.

On Tuesday evening, the agents had an address -- Apartment 202 -- and at 8:30 p.m. a federal judge in Raleigh issued the warrant from his home. At 2 a.m. Wednesday, while a cold rain fell in Raleigh, FBI agents knocked on the door of Apartment 202.

It took Mitnick more than five minutes to open it. When he did, he said he was on the phone with his lawyer. But when an agent took the receiver, the line went dead.

Aleph One / aleph1@underground.org

Last modified Feb 24, 1995.

==========

ALGUNS TERMOS IMPORTANTES DO JARGON:

==========

:brute force: adj. Describes a primitive programming style, one in which the programmer relies on the computer's processing power instead of using his or her own intelligence to simplify the problem, often ignoring problems of scale and applying naive methods suited to small problems directly to large ones. The term can also be used in reference to programming style: brute-force programs are written in a heavyhanded, tedious way, full of repetition and devoid of any elegance or useful abstraction (see also {brute force and ignorance}).

The {canonical} example of a brute-force algorithm is associated with the `traveling salesman problem' (TSP), a classical {NP-}hard problem: Suppose a person is in, say, Boston, and wishes to drive to N other cities. In what order should the cities be visited in order to minimize the distance travelled? The brute-force method is to simply generate all possible routes and compare the distances; while guaranteed to work and simple to implement, this algorithm is clearly very stupid in that it considers even obviously absurd routes (like going from Boston to Houston via San Francisco and New York, in that order). For very small N it works well, but it rapidly becomes absurdly inefficient when N increases (for N = 15, there are already 1,307,674,368,000 possible routes to consider, and for N = 1000 --- well, see {bignum}). Sometimes, unfortunately, there is no better general solution than brute force. See also {NP-}.

A more simple-minded example of brute-force programming is finding the smallest number in a large list by first using an existing program to sort the list in ascending order, and then picking the first number off the front.

Whether brute-force programming should actually be considered stupid or not depends on the context; if the problem is not terribly big, the extra CPU time spent on a brute-force solution may cost less than the programmer time it would take to develop a more `intelligent' algorithm. Additionally, a more intelligent algorithm may imply more long-term complexity cost and bug-chasing than are justified by the speed improvement.

Ken Thompson, co-inventor of UNIX, is reported to have uttered the epigram "When in doubt, use brute force". He probably intended this as a {ha ha only serious}, but the original UNIX kernel's preference for simple, robust, and portable algorithms over {brittle} `smart' ones does seem to have been a significant factor in the success of that OS. Like so many other tradeoffs in software design, the choice between brute force and complex, finely-tuned cleverness is often a difficult one that requires both engineering savvy and delicate esthetic judgment.

:crack root: v. To defeat the security system of a UNIX machine and gain {root} privileges thereby; see {cracking}.

BIBLIOGRAFIA

Algumas partes em ingles mencionadas aqui vieram direto do
The on-line hacker Jargon File, version 3.0.0, 27 JUL 1993".)

Me referenciei muito tambem no "Hacker Crackdown" do Bruce Sterling, que esta' disponivel gratuitamente on-line no ftp site ftp.eff.org no subdiretorio pub/Publications/Bruce_Sterling

A parte da legislacao veio de um arquivo de CDROM contendo softwares brasileiros. Infelizmente esqueci o nome do dito. Sei que tem BBSes que tem o mesmo. O arquivo original tinha mais de 200 kbytes e engloba muita outras coisas.

A parte do Press Release veio do artigo sundevil

Disponivel no ftp.eff.org no
subdiretorio pub/Publications/CuD/Papers

```
{}            ELECTRONIC TEXT -- PUBLIC INFORMATION FILE              {}
{}                      ** SPECIAL EDITION **                         {}
{}                        THE EPIC PROJECT                            {}
```

Press RETURN to Continue: