BARATA ELETRICA, numero 8
Sao Paulo, 20 de dezembro, 1995

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.

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

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

rodrigde@spider.usp.br (liberaram para divulgacao)
informatica-jb da esquina-das-listas@dcc.unicamp.br ou:
wu100@fim.uni-erlangen.de

Correio comum:

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

Numeros anteriores:

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

NO BRASIL:

http://www.inf.ufsc.br/ufsc/cultura/barata.html
ftp://ftp.ufba.br/pub/barata_eletrica

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

  UNITED STATES:
etext.archive.umich.edu in /pub/CuD/Barata_Eletrica
ftp.eff.org in /pub/Publications/CuD/Barata_Eletrica
aql.gatech.edu in /pub/eff/cud/Barata_Eletrica
world.std.com in /src/wuarchive/doc/EFF/Publications/CuD/Barata_Eletrica
uceng.uc.edu in /pub/wuarchive/doc/EFF/Publications/CuD/Barata_Eletrica

wuarchive.wustl.edu in /doc/EFF/Publications/CuD/Barata_Eletrica
  EUROPE:
nic.funet.fi in /pub/doc/cud/Barata_Eletrica
                  (Finland)
(or /mirror/ftp.eff.org/pub/Publications/CuD/Barata_Eletrica)
ftp.warwick.ac.uk in /pub/cud/Barata_Eletrica (United Kingdom)
  JAPAN:
 ftp.glocom.ac.jp in /mirror/ftp.eff.org/Publications/CuD/Barata_Eletrica
 www.rcac.tdi.co.jp in /pub/mirror/CuD/Barata_Eletrica

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

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

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

NO BRASIL:
http://www.inf.ufsc.br/ufsc/cultura/barata.html

==========

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

drren@conex.com.br
wjqs@di.ufpe.br
aessilva@carpa.ciagri.usp.br
dms@embratel.net.br
clevers@music.pucrs.br
rgurgel@eabdf.br
invergra@turing.ncc.ufrn.br

CREDITOS II :
Sem palavras para agradecer ao pessoal que se ofereceu para ajudar na
distribuicao do E-zine, como os voluntarios acima citados, e outros,
como o sluz@ufba.br (Sergio do ftp.ufba.br), e o delucca do www.inf.ufsc.br
q. talvez estao arriscando a ira dos superiores, ao disponibilizar para o
resto dos brasileiros este material. Muito obrigado. Espero continuar
agradando. A propria existencia desse pessoal e' um sinal para mim de que
vale a pena continuar escrevendo, enquanto puder fazer isso). Valeu tambem
o Leandro do Zine Alternetive, que me entrevistou.

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

INTRODUCAO:

Oi, gente. O numero 8 demorou. Quase nao sai. Sinceramente. Provas, problemas financeiros e de habitacao. Sem falar em problemas medicos.Serio. Isso em final de curso. O que a gente nao faz pelos fas. De ferias, to com um pouco mais de tempo, da' pra pensar em fazer algumas coisas. Como pensar na reuniao de hackers.

To virando noticia. Apareci na TV, na Super Interessante, numa entrevis p. Radio Eldorado AM .. so' falta o Jo^ Soares. Um dia, quem sabe? Um amigo me chamou de Anti-hacker, por gana de ficar famoso. Mas tenho que divulgar minha mensagem. So' assim chego la'. E quero fazer o pessoal no Brasil se reunir, trocar ideias, aprender em conjunto. Fazer uma Hacker Conference no pais.

Falando nisso, recebi e-mail de Recife. Nada mais nada menos do que o primeiro rato de computador pego fazendo break-in. Nao me deu permissao pra usar a carta dele e respeitei. Parece que a captura dele foi bem mais elaborada. Ou pelo menos e' o que fala. De acordo com ele, a VEJA publicou uma versao inteligivel, porem fantasiosa, da coisa. Nao falou do acesso root e umas coisas mais. Fiquei contente em saber que pelo menos o e-zine chegou ate' la'. Dei para ele o direito de escrever se defendendo, ele recusou.

Mas mudando de assunto: e o Sivam? Sei la'. Tenho uma opiniao formada sobre esse escandalo. E nao vou comentar. E' coisa do governo. Falando em governo, tem um otimo texto do Henry David Thoreau:

> "The mass of men serve the state thus, not as men mainly, but as machines, with their bodies. They are the standing army, and the militia, jailers, constables, posse comitatus, etc. In most cases there is no free exercise whatever of the judgement or of the moral sense; but they put themselves on a level with wood and earth and stones; and wooden men can perhaps be manufactured that will serve the purpose as well. Such command no more respect than men of straw or a lump of dirt. They have the same sort of worth only as horses and dogs. Yet such as these even are commonly esteemed good citizens. Others--as most legislators, politicians, lawyers, ministers, and office-holders--serve the state chiefly with their heads; and, as the rarely make any moral distinctions, they are as likely to serve the devil, without intending it, as God. A very few--as heroes, patriots, martyrs, reformers in the great sense, and men--serve the state with their consciences also, and so necessarily resist it for the most part; and they are commonly treated as enemies by it."

Sem duvida um pensamento radical. A todos voces, um feliz Natal.

INDICE:

BATALHA PELA MENTE

E' uma coisa dificil de explicar. Quando voce consegue entender.. fica dificil aceitar. Sua vida muda. A cabeca gira. E o mundo da' voltas. Mas existe. Como e' muito complicado, vamos por partes (Jack The Ripper).

Como definir o que e' a realidade? Vamos analizar em um nivel bem basico: se voce esta' lendo este texto, esta' usando os olhos, certo? Se esta' lendo no micro, esta' tambem usando o teclado, caso contrario pode ou nao estar usando as maos. Pode sentir pelo tato que esta' ou nao segurando o texto. Mas tem um detalhe a mais. O texto esta' em portugues e voce sabe ler. E esta' curioso sobre o conteudo. Por isso continua lendo. Se concorda ou nao concorda, e' indiferente. Talvez o meu texto consiga prender sua atencao ate' o final. Talvez voce tenha um compromisso e deixe o texto para mais tarde. Em outras palavras, nao e' algo importante. De qualquer forma, uma coisa voce tem razoavel certeza. Este texto existe. Nao e' produto da sua imaginacao.

Vamos supor que o papel que contem este texto desapareca. Seu irmao ou irma pegou. Pior, formataram o disquete. E sua conta Internet esta' bloqueada. Para piorar o quadro, ninguem nunca ouviu falar do e-zine Barata Eletrica. Nem seus amigos se lembram de ter ouvido voce comentar sobre este zine. Pronto. Voce nao tem como saber se este artigo aqui nao faz parte de sua imaginacao. Daqui a algum tempo, talvez ele nao faca diferenca, ficou perdido em algum canto esquecido da memoria.

Vamos agora pegar uma noticia na TV. A TV, como voce sabe, e' uma caixinha de Pandora. Pode-se escolher o canal que se quer assistir e dependendo do horario, ouvir e ver as noticias. Mas o que aparece la' nao e' necessariamente o que esta' acontecendo agora. O que esta' la' e' fruto de um esforco em equipe, onde um sujeito, o reporter, foi ao local do acontecimento, junto com um cameraman, eles juntos filmaram um evento, a fita foi editada, enviada para a estacao de TV, para ser transmitida, apos um anuncio por outro reporter, que e' o chamado "ancora" da estacao. Nao e' um sujeito que por telepatia sabe a noticia e relata ao publico. Dependendo da reportagem, se composta de duas testemunhas, voce escuta as duas testemunhas. Vamos transportar isso para algo mais simples.

Se voce escuta uma fofoca, voce esta' ouvindo o relato de uma pessoa que te contou uma parte da noticia. Qualquer duvida, voce fara' questao de escutar a outra pessoa envolvida. E' uma noticia, mas como e' contada por outra pessoa que pode ou nao ter interesse na coisa, talvez tenha contado errado, talvez sei la'. Ao contrario da TV, fofoca e' uma coisa que a gente sempre duvida. Todo mundo sabe que "quem tem conto aumenta um conto". Mas vamos voltar ao lance da nocao do mundo real.

Uma pessoa presa numa cadeira de rodas, um paraplegico, daqueles que so' pode ficar na frente da televisao, mas pode ouvir e falar, mas nao tem telefone. A nocao de mundo que o cara tem esta' entre quatro paredes. Toda a informacao nova dela depende das pessoas que o visitam. Se a gente coloca o cara num hospital, a realidade dele e' dormir, acordar, comer, e um nada qualquer o resto do tempo. Numa ilha deserta, sem ninguem, talvez nem isso.

Okay. Ta' muito metaforico, isso. Vou colocar uns fatos. Existe uma experiencia famosa, feita no MIT, sei la' quanto tempo atras. Na colecao "Biblioteca Cientifica LIFE", livro de Psicologia, da' pra se checar a informacao. Sintetizando, alguns voluntarios foram colocados em salas de isolamento total. Nao se ouvia nada, nao se via nada, ninguem conversava com os caras. Alguns dos estudantes aguentaram as 24 horas do experimento. Na saida da sala, alguns teste. Um dos caras ficou um tempao tentando equilibrar um cigarro em cima de uma mesa. E'. Um cigarro. Nao, o cara nao tinha puxado um fumo ou ficado bebado durante a experiencia.

A conclusao a que os caras chegaram e' que .. comer, beber, dormir, respirar, nao e' so' o bastante pra viver. As pessoas precisam de um "input", uma entrada de informacoes constante, diariamente. Quando voce anda na rua, existem centenas de informacoes que sao analizadas pelo cerebro: seu nariz interpreta cheiros, sua pele sente o contato da roupa, ha' barulhos que compoem o seu ambiente. Quando nao existe este "input", voce degenera. A NASA, quando treina seus astronautas para viagens espaciais tambem inclui esse tipo de experiencia de isolamento. A pessoa, desprovida por longos periodos de inatividade ou ausencia de sensacoes, alucina, da mesma forma que uma pessoa numa sessao de LSD.

Okay. Vamos voltar ao cotidiano. As pessoas precisam esse impulso, essas sensacoes, vem de fora da pessoa, nao de dentro. O ambiente em que voce influencia sua cabeca. Todo mundo pode acreditar no que quiser, mas seus pensamentos, suas lembrancas, sao formadas em parte de coisas cuja importancia o cerebro aprendeu a ignorar. Isso da' muito material de discussao, mas o fato onde quero chegar e' que a maior parte das pessoas nao se da' conta dessa quantidade de informacao porque ela e' manipulada a nivel do inconsciente. Se voce sente um cheiro que nao gosta, o cerebro te avisa para voce poder tomar uma decisao e sair longe do cheiro (por exemplo). Na verdade, no caso especifico do olfato, essa sensacao so' dura 30 segundos, depois tende a desaparecer.

Como disse, isso acontece a nivel inconsciente. A mesma coisa acontece a nivel de imagem e de som. Se voce reagisse a todo tipo de imagem e de som, ir a um concerto de rock ou assistir TV era impossivel. Isso so' acontece porque o cerebro fica "indiferente" a um grande numero de imagens. Alias, aquilo que voce pensa que e' um filme, sao fotos expostas a razao de 24 quadros por segundo. O cerebro consegue "ver" cada uma das fotos, mas acaba so' analisando as diferencas, o que da' uma sensacao de movimento.

A nivel psicologico, o cerebro nao e' so' dividido entre o consciente racional e o inconsciente. Existe tambem uma terceira parte, que e' o produto da nossa interacao com o meio ambiente e sociedade. Por exemplo: eu gosto daquela pessoa. Entao ao ve-la, automaticamente sorrio e falo alguma coisa boa. Nao e' algo exatamente automatico ou treinado, mas e' um gesto aprendido e ensaiado. Se a pessoa esta' com a cara amarrada, nosso cerebro analisa a informacao. Por isso emite uma resposta como: " esta tudo bem?", mesmo que a pessoa nao comente nada.

Interessante, ne'?

Quer um pouco mais? Se voce se veste de forma errada, vamos supor que tem uma coisa nas suas costas. As pessoas talvez nao falem nada, mas voce vai sentir algo errado. Entendeu o principio da coisa? Isso e' voce respondendo a um estimulo inconsciente. Mas num jogo de futebol, por exemplo, existe o drible, antes de chegar no gol. O atacante faz todo um jogo para que o goleiro pense que a bola vai chegar num lugar diferente. Estimula uma reacao do goleiro, que pula num lugar diferente. A isso pode se chamar de varios nomes, mas estou colocando como exemplo de "manipulacao do inconsciente".

Uma forma de analisar esse lance, e' observar comerciais de TV. Ninguem chega pra voce e fala que cigarro e' bom. Mesmo fumantes vao lhe dizer isso, embora o vicio seja uma coisa dificil de largar. Mas o que mostra uma propaganda de cigarro, por exemplo. Gente com um sorriso enorme no rosto. Situacoes parasidiacas, mulheres maravilhosas, sorridentes, em

lugares como praias, gente embaixo d'agua, etc coisas que a grande maioria de nos, que trabalha das nove as cinco ou estuda, nao pode fazer. E aqui e ali, as cores da marca de cigarro. Mas veja bem: isso nao acontece uma unica vez. E' repetido N vezes. A maioria das pessoas nem repara nos detalhes de um comercial. Mas o corpo, este sonha com um descanso longe do escritorio que tem o ar condicionado quebrado. E talvez a pessoa sonhe com uma mulher com metade do corpo dquela manequim. Como disse, e' uma tentacao, mas nao e' uma unica vez que o comercial passa. Sao muitas vezes e .. opa! A pausa para comerciais comeca exatamente naquele minuto X em que a acao se desenrola no filme. E'. Entao, o comercial e' passado num instante em que, teoricamente seus olhos deveriam estar bem abertos.

Voce pensa que e' so' na televisao que isto acontece? Na, na, na, nao. Isso acontece em revistas. Alias, o preco que voce paga por uma revista em banca nao e' o que sustenta o trabalho de se fazer a dita. Sao os anuncios. Algumas revistas sao metade anuncio, o texto e' uma forma de chamar a atencao para os produtos a venda. E de certa forma, o sujeito acaba tomando conhecimento dos artigos expostos. Sim. Nao precisa que todo mundo ao mesmo tempo preste atencao. Basta que as revendas saibam da existencia do produto. Se as revendas compram, nao importa que o fulano que le a revista compre. No momento em que ele decidir ir na loja e digamos, comprar um tenis qualquer, o que saiu na revista esta' com preco mais caro e mais a vista, exatamente porque o dono da loja comprou de alguem e quer ver uma grana p. garantir o dia-a-dia dele.

Nao e' so' isso. Junto com a propaganda do Tenis, existe uma tematica associada. Entao o sujeito que compra o tenis, que por exemplo, o Mike Tyson diz que usa, por um jogo mental, se sente importante quando ve o comercial na TV. Por exemplo. Os amigos, que nao tem grana p. comprar o tenis, ficam com inveja, porque nao podem ter a mesma sensacao. O comercial e' uma lembranca clara "voce e' pobre". Existem comerciais que se dao conta disso e colocam que "nao e' o produto que e' caro, e' voce que ganha pouco", e por ai' vai. As empresas de propaganda trabalham com segmentos de mercado e ganham rios de dinheiro, exatamente porque sabem fazer batalhas em que conquistam o comprador, de forma consciente ou subconsciente. Facilitam a venda de um produto. Fazem com que o sujeito redefina todo o seu modo de vestir, num movimento chamado "moda" e se sinta inadequado sem ela. Nao que sempre tenham sucesso fazendo isso. Claro que as pessoas gostam de um comercial bem-feito. Ele foi feito para despertar uma simpatia por um produto. Tudo bem que a loira que anuncie aquela bebida na vida real nao saiba nem como assoar o nariz em publico (o ideal e' pedir licenca e assoar no banheiro, por falar nisso). Na propaganda ela e' a imagem da tentacao que o anunciante quer que o produto tenha.

Isso acontece a nivel de filmes, tambem. Todos os jornais falam mal da CIA, por exemplo. Mas filme de espionagem e' algo sempre excitante, tem um mocinho e um bandido. E o bandido e' feio, cospe no chao, come criancinhas, etc.. As pessoas tendem a acreditar na ideia de que existe um bem e um mal. Procuram gente para assumir estes papeis. Pois bem, o cinema pode manipular de forma a tornar determinada imagem mais cosmetica. Antes da guerra do Vietna, pululavam filmes de guerra. Porque? Porque volta e meia, os EUA entravam em guerra ou mand(av)am seus fuzileiros navais pra algum lugar. E nao e' facil convencer alguem a mandar seu filho de 18 anos para ir morrer, num lugar sei la' onde. Ah, sim. Os filmes costumam ter cenas em que aparece uma mulher, enfermeira, oficial ou coisa que o valha, para que as mocas que vao assistir a fita nao se sintam ignoradas. Pode ser ate' um filme como Spartacus (do Stanley Kubrick). Tem uma historia de amor. Ou Rambo II, a vinganca. Talvez por isso nao se faca filme de guerra, no Brasil, entre outras razoes. Guerrear quem?

Aonde eu quero chegar com tudo isso? Nao quero chegar muito longe. Se voce leu ate' aqui e' sinal de que consegui prender a sua atencao. Alguma coisa voce absorveu. Provavelmente, cedo ou tarde isso vai voltar a sua cabeca e sera' objeto de divagacao, quem sabe. E' ai' que eu queria chegar.

A REDE - O FILME E SUAS METAFORAS

Aqueles que tiveram sorte me viram falando na TV no jornal do SBT, dando um opiniao sobre o filme "A REDE", em cartaz na cidade de Sao Paulo. E' um daqueles casos em que o roteirista parece ter trabalhado em algum jornal do tipo "Noticias Populares". O filme, que tem ate' uma pagina na Web, carrega uma mensagem muito simples: voce pode ser vitimado pelos hackers se mexer com software "proibido". Tem gente muito melhor do que eu enumerando os erros do filme, mas e' essa a mensagem basica. Tudo no filme e' exagerado ao extremo para construir um personagem, um simulacro de pessoa que deixa de existir, por acao de um grupo de gente que ela nunca viu na vida, mas que detem o acesso a uma "porta dos fundos" de um software de vigilancia. Pra encurtar a historia: a menina e' especialista em virus, bugs e problemas que pintam em programas recem-lancados no mercado (pelo visto, so' pra programas p. computadores Macintosh). No dia em que ela sai de ferias, mandam um programa p. ela que tem um cavalo-de-troia ou que acessa uma porta-dos-fundos do sistema mais comum de vigilancia (tipo firewall ou trip-wire) em uso. O cara que enviou o disquete morre num acidente de aviao, cujo sistema de navegacao foi adulterado. Primeira manipulacao de computador. La' no lugar onde ela veraneia, no ultimo dia, conhece um cara que na verdade e' pertencente ao grupo responsavel pelo programa.

Pinta uma cena digna de novela da Globo e depois dessa, ela ta' num hospital sem os documentos, vai voltar pros EUA e comeca a descobrir que nao existe mais. Ou melhor, ate' existe, mas outra pessoa tomou o lugar dela. E a identidade que sobrou e' de alguem condenado por roubo, trafico, prostituicao, etc.. Ai', a unica pessoa que sabe quem ela e', e' um ex-namorado. Que ajuda-a com roupas e o basico para recomecar a procurar sua identidade, ja' que a casa dela foi vendida. Atraves do amigo, a mae dela, que sofre de amnesia senil, e' transferida para outro lugar. O amigo, sofre um problema medico, e' internado, recebe o medicamento errado e morre. Presa, teria que assumir a identidade falsa p. ter chance num julgamento, ou seria julgada como louca, alem de estelionataria e prostituta.

Ela descobre ao longo do crime que existe uma organizacao criminosa, especie de "milicia" que esta' tentando se apoderar do poder atraves desse software, que seria tudo aquilo que a midia propagandeou que o SATAN permite fazer, dar acesso ilimitado a qualquer computador. Roda em MAC, inclusive. E e' essa milicia, representada pelo cara que paquerou-a nas ferias, que a persegue no filme inteiro. No final das contas, ela recupera a identidade, ao invadir um computador do governo e colocando nele um virus que apaga tudo.

O filme tem umas sacadas interessantes, cativa. Mas o tempo todo esbarra em montes de coisas que nao tem nada a ver com a realidade. Mesmo la' nos EUA, nao e' tao facil mexer com a identidade de uma pessoa. Porem, pode ser interessante criar um tipo de acao onde isso seja possivel para justificar aquilo que o governo americano costuma fazer com aqueles que sao suspeitos de mexer com computadores do governo. O Chris Googans, da revista Phrack, deixou bem claro no seu discurso, no congresso de Hackers la' na Inglaterra. "Nao facam acesso ilegal nos EUA". Existem leis severas e mesmo que o cara nao saia preso, com certeza vai ser vigiado pelo resto da vida. Qualquer pessoa suspeita de mexer com acesso ilegal e' vigiado ate' que cometa algum crime. Ai' os caras enviam tudo, ate' helicoptero, equipes de SWAT na casa do sujeito. E'. Nao e' exagero. Claro que de vez em quase sempre, a pessoa "suspeita" de hacking tem catorze anos. Gente mais velha sabe como evitar ser descoberta e nao se mete a fazer besteiras. So' para se ter uma ideia, ha' muita, mas muita gente que duvida que o Mitnick seja responsavel pelo break-in no computador do Shimamura. Mas isso e' outra historia.

Bem verdade que la' existe facilidade de acesso aos dados de qualquer um. E' quase tao facil quanto comprar um CDROM. So' que CDROM's, por exemplo nao sao apagaveis. Nao existe um software que "grave um CDROM" se o drive for apenas de leitura de CDROM, que e' o que acontece com os drives multimidia atualmente vendidos. Durante um tempo foi estocado em varios sites da rede, um software que prometia isso, mas era um cavalo-de-troia que destruia o disco rigido de quem pensasse que poderia gravar coisas em CDs. Da mesma forma, existe o mito de que hackers possam "brincar" com a identidade alheia. Besteira. Consultar sim, isso e' possivel. Alterar, so' as autoridades competentes. Talvez hajam casos em que atraves de propina, isso seja possivel. Engano de identidade, sim. Existe gente que ja' cumpriu pena por que foi confundida com outra pessoa. Mas isso sao outros quinhentos.

E' possivel isso acontecer aqui no Brasil, as pessoas saberem tudo a seu respeito? Claro que e'. A pessoa que tem uma faxineira que vem uma vez por semana simplesmente "confia" toda a sua privacidade a alguem desconhecido. Ficou famoso o ano passado as historias de "faxineiras" que eram ladras. E em caso de sequestro isso tambem acontece. Essa coleta de informacoes nao e' feita por computador. Cursos de detetive por correspondencia ensinam como isso e' feito. Basta entrar numa agencia de correios e telegrafos. E existem conversas com pretexto, atraves do qual voce motiva a pessoa a revelar coisas importantes atraves de perguntas muito sutis. Os "hackers" chamam isso de Engenharia Social, mas e' uma forma sutil de interrogatorio. Quer saber dos problemas financeiros do fulano? Pergunta que que ele acha de comprar tal aparelho de som ou equipar seu computador com um multi-midia. Quer perguntar p. sua amiga se o namorado dela e' bom de cama, mas nao tem intimidade p. tanto? Comenta com uma terceira pessoa, na frente dela, que o sujeito parece meio inexperiente ou "desajeitado". Logico, se voce pergunta isso num IRC, a coisa fica mais complexa. Tem muita gente que nao se controla e ate' revela ate' o que a gente nao pergunta. E obvio, existem muitos, mas muitos truques para se avaliar uma pessoa.

E' possivel a pessoal "tomar" sua identidade? E' meio estranho pensar que alguem consiga fazer qualquer coisa com os bancos de dados que existem sobre o cidadao. O cadastro da pessoa fisica, vulgo CPF, era inicialmente (se nao me engano) para movimentacoes financeiras somente. Embutido no numero do CPF existe uma formula matematica que permite avaliar se o numero e' mesmo da pessoa. So' que ja' houve escandalos com politicos tendo mais de tres numeros de CPF. De acordo com reportagem da Folha de Sao Paulo (6/11/95, 1-8), existem 7 milhoes de pessoas com o mesmo nome, 3 milhoes tem o mesmo nome e data de nascimento, 2 milhoes ainda nasceram no mesmo municipio, 42.200 se chamam Maria Jose' da Silva, 28.900 Maria Aparecida da Silva, 21.200 Jose' Carlos da Silva, etc.. Meu nome, que e' D-E-R-N-E-V-A-L, nao Demerval ou Denerval, tem varios na minha cidade, inclusive com sobrenome semelhante (Aqui em Sao Paulo, e' relativamente incomum, quando tirei minha carteira de trabalho, o sujeito me falou que D-E-R-neval era o primeiro que conhecia, em 28 anos de Ministerio do Trabalho), isso por exemplo. Ja' ouvi falar do caso de um sujeito que criou um cartao de credito com o nome de um milionario e usou como se fosse seu. Foi preso. Existem tambem casos de criminosos que ao matar a vitima, usam os documentos dela como se fossem seus. Ja' ouvi falar de gente que foi atropelada por policiais e que foi despojada de todos os documentos antes de ser entregue no Pronto-Socorro. Se morresse, seria enterrado como indigente. Desapareceria, em outras palavras, mas a familia procurou em tempo. Houve o caso famoso tambem de um sujeito, no Rio Grande do Sul, que viajou sem avisar e a mae reconheceu o cadaver de outra pessoa como seu. Na verdade, o cara tinha deixado um bilhete, que caiu no chao, foi varrido e iniciou a historia toda. Custou uma nota preta para desfazer. Virou ate' "Caso Especial" da Globo.

Aqui no Brasil, quando alguem nasce, normalmente recebe um atestado de

batismo, em alguma Igreja, e' registrado em Cartorio, num livro com paginas numeradas e que nao pode ser rasurado ou alterado. Tem tantos documentos que nem vale a pena comentar. A prefeitura de Sao Paulo por exemplo, estava lancando uma carteirinha de identificacao p. estudante primario. Tem a carteirinha da UNE, da UBES, tem o titulo de eleitor, etc. Nenhum desses servicos e' informatizado ainda. Sao papeis. Existe ou existia em Sao Paulo durante a ditadura (pode ter acabado) uma praca onde o sujeito podia "encomendar" para "despachantes", todo um conjunto de documentos falsos, por preco modico. Alias, com jeitinho, ate' alguns anos atras, era possivel "comprar" carteira de motorista falsa no Rio de Janeiro. O funcionalismo publico e' mal pago e o trabalho e' feito de forma arcaica. Tanto que existe a possibilidade de obter anulacao de casamento quando existe "erro de pessoa".

Ta', isso nao responde se alguem poderia realizar na vida real, aquilo que foi feito no filme. Que que acontece quando sua carteira e' roubada? Voce tem que imediatamente produzir um boletim de ocorrencia na delegacia mais proxima. Se tiver um cartao de credito, telefonar para o numero indicado quando voce assinou os documentos e cancelar o(s) cartoes. O mesmo e' valido para taloes de cheque. O boletim de ocorrencia deve ser levado para o banco para sustar o pagamento dos cheques. Depois e' comecar o processo de reconstruir seus documentos. Leva tempo. Ja' ouvi falar de gente que foi roubada no centro de Sao Paulo e que pode "recomprar" os seus documentos, perguntando pra Deus e o mundo perto do local do assalto se os mesmos nao haviam sido encontrados. O desespero faz o milagre.

Fazer as coisas On-line, isso so' no filme. Existe o SERPRO, Servico Federal de Processamento de Dados em Sao Paulo, que centraliza as informacoes. Existe um processo de modernizacao em andamento, mas essa centralizacao significa atender milhares de micros. Num sistema tao lento, qualquer consulta leva tempo.

O que funciona On-line sao informacoes bancarias. O que torna o sigilo bancario algo essencial. Quando voce usa um cartao de credito, ele pode ser copiado por um funcionario. Existem "fabricas" clandestinas que confeccionam cartoes de credito falsos, mas identicos em quase todos os detalhes, ao cartao original. Isso foi materia de televisao ha' nao muito tempo. Houve um escandalo, em 94, acho, quando uma empresa que fabricava cartoes eletronicos tinha um grupo de funcionarios corruptos fazendo copias dos mesmos. Da' medo de entregar o cartao de credito para alguem. Mas isso nao e' tudo. A pessoa, quando compra algo com o cartao de credito paga uma fatura. Isso fica registrado. Nos EUA esse registro e' usado para se avaliar alguem, num emprego. La' todo mundo usa cartoes de credito. Se as pessoas sabem o que voce compra, sabem a sua personalidade, sabem quando voce atrasa suas contas, sabem quanto voce ganha. Quando voce escreve, aqui no Brasil, no verso do talao de cheques, onde voce mora (coisa que ja' me falaram ser uma frescura sem fundamento legal, teoricamente o numero do telefone e R.G. seriam suficientes p. identificacao) esta' liberando informacao a seu respeito. Afinal, com o RG, o CPF (que fica no talao de cheques) e o endereco, ja' se pode fazer muita coisa. O ideal e' sempre comprar usando dinheiro vivo e se recusar a comprar com cheque principalmente se pedirem o endereco no verso do talao. Por mais "coisa de pobre" que isso possa parecer. Com gente sendo morta por nao entregar a senha do cartao eletronico, tambem pode ser inteligente nao sair com o dito. Mas e o uso "fraudulento" dos seus dados?

Um exemplo que ja' soube foi o caso de uma ex-namorada de um sujeito. Ela sabia que o cara estava dia tal, hora tal, no apartamento dele. Com outra garota nova. Encomendou um jantar completo no Golden Room do Copacabana Palace a ser entregue la'. Entregou o RG do cara p. legalizar a compra. Legal, ne'? O sujeito nao tinha tanto dinheiro assim.

Outro exemplo e' entregar o numero de telefone p. qualquer um. Tem gente que fica sabendo e coloca um desenho de um ser humano de quatro no chao, com os dizeres: "Quase um Martini. Em qualquer hora, em qualquer

lugar, com qualquer um". Ta' certo que revista erotica, hoje, nao aceita mais "anuncios eroticos" sem um pseudonimo e caixa postal, mais xerox de documentos e comprovacao de aluguel de caixa postal, senao eu iria colocar outra forma de usar o endereco de outra pessoa. Motel e' outro exemplo de lugar que se preocupa com o anonimato das pessoas. Voce entrega a carteira de identidade para alugar um quarto. Mas vamos voltar a Internet.

Uma coisa que costuma pintar as vezes, tanto no IRC quanto no correio eletronico, nao sao apenas as pessoas que sabem muito a seu respeito. Ja' falei sobre isso num artigo anterior. Obvio, se voce frequentemente envia cartas p. o grupo Usenet tal, tal e tal, pessoas que frequentam tais grupos ja' tem uma ideia do seu gosto. E' possivel checar via programa ou ate' melhor, via e-mail, conseguir uma relacao de cada pessoa que posta cartas para newsgroups. Isso sao dados que podem ser usados para compor uma identidade virtual da pessoa. O Sysop do lugar onde voce tem conta internet pode fazer uma estatistica de quais programas voce acessa e por quanto tempo. A pessoa tem a ver com os Newsgroups e listas de discussao nas quais esta' inscrito ou se corresponde.

Claro que a pessoa com quem voce se corresponde no IRC, naquele tao falado "namoro eletronico" pode nao ser o mesmo que voce acha que e'. Tem muita gente que usa pseudonimos (nickname) de sexo diferente de vez em quando, para experimentar ou ate' mesmo casos de criar um grupo de discussao com varios nicknames dos dois sexos, para atrair outras pessoas para a discussao. Existem formas de se esconder a identidade real (endereco e-mail). E ha' varios subterfugios para se enganar a pessoa com quem se fala. E' preciso ser hacker para se saber isso? Nao, qualquer pessoa que fuca muito, pergunta e se informa, acaba sabendo. Uma piada muito comum e' a do sujeito que comeca a receber correspondencias de uma menina que se assina "gatinha dengosa". Essa e' do tempo em que o Video-texto comecou. O sujeito comecava a se corresponder com um cara, falando o diabo. "Sou loira, olhos azuis, mas me acho muito feia", "Gosto de lidar com computadores", "Odeio gente que so' sabe falar de futebol", "Suas cartas me ajudam muito a compreender o assunto", "Imagino voce lindo, quero te conhecer". Esse tipo de correspondencia. E isso e' um cara enrolando o outro. Um dia um sujeito veio pedir p. passar na frente dele, para usar o terminal, na epoca comum em grandes shoppings, como o Eldorado (cheio de fila tambem). O motivo? Ver a cartinha que a "namorada eletronica" deixou para ele. Eu mesmo ja' parei de contabilizar o numero de pessoas que aparece do nada, e quer trocar correspondencia.

Uma vez mantive correspondencia com uma. Mas tinha certeza razoavel da identidade "feminina". Pedi a uma amiga minha p. ler as cartas dela. Costuma funcionar. Uma mulher sabe quando e' outra mulher que esta' escrevendo. Tambem sabe quando a mulher ta' enrolando ou falando a serio. Quando se tem um pouco de idade, pode-se saber quando outra pessoa esta' enrolando ou falando a serio. Por isso, tem correspondencias que para mim, sao exercicio de enrolacao, nada do que falo e' 1) objetivo, 2) informativo, 3) serio, 4) inteligente. Correspondencia a serio, depende muito da pessoa. Existe namoro eletronico, isso existe. Conheco gente que ja' se encontrou no IRC, que nem aconteceu no Globo Reporter e na (argh!) novela da Globo. Existe um newsgroup para isso, o alt.romance, se nao me engano. Uma menina que postou anuncio de namoro la' recebeu cerca de 400 propostas. Deve ser bom p. levantar o moral de alguem. Ou para encher a caixa postal de uma pessoa com junk-mail. Ah, sim. Fazer uma carta falsa e' um dos truques mais simples da Internet. E' uma das razoes pelas quais gente importante, tipo o presidente dos EUA tem uma especie de codigo que vai no subject: para identificacao. Se voce mandar um fake-mail para ele como se fosse uma pessoa da familia dele, sem o codigo, a correspondencia sera' ignorada.

Mas ha' algumas formas de ter seus dados devassados, atraves da rede. Varias mensagens que estao aparecendo no newsgroup Sci.crypt e Comp.risks, alertam para o fato de que o Win95 e' um paraiso para "crackers". Nao vou

colocar a lista, mesmo porque posso fazer depois um artigo em cima do assunto, mas alem do "espiao" que mencionei em artigo anterior (que ja' abre um leque de possibilidades), existem bugs no sistemas de acesso a rede Internet do sistema operacional que permitem a alguem de fora invadir o seu micro enquanto voce usa a rede.

Bill Gates, no seu livro "A Estrada do Futuro", coloca bem claro o que ele pensa do assunto: "Seu micro de bolso sera' capaz de registrar audio, hora, lugar e ate' video de tudo o que acontecer com voce. Sera' capaz de gravar cada palavra que disser e cada palavra dita a voce, bem como temperatura corporal, pressao sanguinea, pressao barometrica e uma variedade de outros dados sobre o ambiente ao seu redor. Sera' capaz de controlar todas as suas interacoes com a estrada (de informacoes) - todos os comandos que voce emitir, as mensagens que enviar e as pessoas para as quais voce ligar ou que ligarem para voce". Em outras palavras, como disse a Barbara Gancia do jornal Folha de Sao Paulo "George Orwell e' pinto perto de Bill Gates. Existe uma versao mais completa na revista Veja de 18/11. Mas o fato e' que: se alguem roubar seu micro de bolso? Se alguem xerocar os dados do seu micro de bolso? Se alguem alterar os dados do seu micro de bolso? Ai' sim, nesse futuro, "The Net" se torna mais real. O livro "1984" tambem.

Finalizando: o filme e' um bom thriller. Emociona, aquela coisa toda, as cenas de acao sao interessantes. Mas em termos de vida real, e' uma historia da carochinha. Tudo bem que a pessoa corre riscos a sua privacidade, usando a Internet. Mas isso sao riscos para os quais a pessoa poderia estar preparada para enfrentar, se tivesse um pouco mais de cabeca, e nao fizesse algumas besteiras. Nao e' porque alguem consegue uma conta na Internet que ira' ter toda a sua vida devassada e sujeita ao tipo de coisa que acontece nos filmes. Isso pode acontecer independente de se ter ou nao uma conta Internet. Pode ser que se for encontrada na conta um software "estranho", tipo Satan ou coisa do genero, haja algum tipo de perseguicao por causa do Sysop. Mas quem e' inteligente, nao mexe com isso no computador dos outros. E' so'.

CAOS COMPUTER CLUB

Quando fui na Europa, fiz questao de ir conhecer esse pessoal. Sao uma das mais antigas associacoes de tarados por micro da Europa, com vario grupos em cidades famosas da Alemanha. Se reunem todas as tercas-feiras, para discutir sobre seguranca informatica, novos avancos em telecomunicacoes e computadores, de forma geral. Na verdade, os tempos de "cracking" ja' ficaram para tras e o grupo virou uma coisa ja' do Sistema, ajudando a empresas como instituicoes bancarias a desenvolver sistemas mais seguros e dificeis de serem "crackeados". Sao muito melhores do que gente saindo da Universidade, pelo simples fato de que fazem isso por prazer, nao por obrigacao.

Eles publicam um folhetim, o "Datenschleuder - das wissenschaftliche Fachblatt fuer Datenresende". Ou Datenschleuder sozinho. Catapulta de dados, para quem nao sabe alemao. Na verdade, o inicio do grupo foi interessante. Comecou em Berlim, dividida em duas, com um monte de grupos "alternativos" pela defesa do meio-ambiente, contra intervencao americana na America Latina, etc. Havia muitos grupos de acao e muita imprensa alternativa. Eles comecaram a publicar alguns artigos sobre Hacking e seguranca de dados, coisa bem trivial. Depois que um artigo atingiu uma revista de grande porte, eles foram tao procurados que praticamente foram obrigados a iniciar a publicacao do seu zine. O interesse pelo assunto era muito grande. Como um grupo, discutiam virus de computador, break-ins, fraude telefonica, etc. Eles receberam muita publicidade, principalmente

quando provaram a possibilidade de manipular o sistema bancario da epoca para conseguir dinheiro. Essa valeria a pena escrever um artigo, mas p. simplificar, eles nao desviaram dinheiro, fizeram uma manipulacao bancaria semelhante as que eram feitas no tempo do "Open Market". Com a diferenca de que eles nao tinham o capital que investiram. Era algo que podia ser feito eletronicamente e bastante simples. Apesar das boas intencoes e da divulgacao que fizeram a imprensa, a policia insistiu em vasculhar os escritorios da mocada.

Outra foi a invasao de um computador da NASA. Essa foi um pouco mais ousada. Nao existe so' a rede Internet. Existem redes de computadores que trocam dados entre si, atraves de modem, que nao sao acessiveis via Internet. A Internet comecou com uma rede de computadores que deveria ser forte o bastante p. suportar a perda de varios elos da corrente de comunicacao. A FIDONET e' outro exemplo de rede de computadores interligados, que ate' alcanca a Internet, mas que tem o seu proprio trafego de mensagens. Da mesma forma, grandes empresas que usam computadores tem seus proprios sistemas de mensagens e coneccoes, algumas vezes usam coneccoes proprias. A NASA tem a sua rede de computadores, a DECnet. Mas como toda a rede, sempre exite um elo mais fraco. No caso, era um computador fora dos EUA. O pessoal do CCC conseguiu o acesso a um deles e usou este computador para colocar um cavalo-de-troia no computador americano. O mais interessante e' que atraves do cavalo-de-troia, eles podiam nao so' criar suas proprias contas no computador da NASA, mas usar o mesmo sem serem descobertos. Acabaram aparecendo quando um funcionario desconfiou e resolveu fazer uma estatistica do uso da maquina em determinado momento. E descobriu que, embora ninguem estivesse usando programas em quantidade o bastante, X por cento da capacidade da maquina estava sendo usado. O pessoal do CCC resolveu contar a imprensa o que tinham feito, como uma forma de garantia de que ninguem ia aparecer morto ou coisa do genero. Vale lembrar que havia tropas americanas em quantidade na Alemanha, naquela epoca e isso seria visto como crime de espionagem. Mas o uso nao foi malevolo, nao houve destruicao de dados ou venda posterior de segredos.

Outra coisa foi aquilo que foi descrito no livro "Cuckoo's Egg" do Clifford Stoll. Um hacker alemao, conhecido do grupo, resolveu usar seus conhecimentos para vasculhar computadores americanos de defesa e vender essas informacoes para os sovieticos. Apareceu morto em circunstancias misteriosas. Muito misteriosas. A "filial" do CCC em Hamburgo vende uma copia dos papeis relatando o encontro do cadaver. Provavelmente ainda vou escrever sobre o caso.

Mas tudo isso sao aguas passadas. Hoje, o CCC nao se envolve com ilegalidades de qualquer especie. As vezes, recebem telefonemas, relatando "fiz isso la'", etc. Mas os participantes das reunioes semanais, sempre regadas a "Mehrwegflaschen" de Coca-cola (coca-cola de litro), bebida predileta da mocada, sao algo impressionante. De vez em quando parece luta-livre, gente pega gente pelo pescoco, literalmente, mas na camaradagem. Uma pseudo-agressividade. Fiquei impressionado de descobrir que quando vao a congressos de Informatica, em cada palestra, um membro e' escalado para fazer um resumo da coisa, que e' depois arquivado para uso no fanzine ou sei la', consulta posterior. Conversei com varios integrantes e o pessoal tem as origens mais variadas possiveis: o Andy e' estudante de jornalismo, mas tem gente de Eletrtecnica, ate' Economia e Administracao. Gente de varias idades. Tinha umas vinte pessoas, no dia em que fui la', isso porque o pessoal estava de ferias e alguns tinham viajado. A grande preocupacao do grupo e' a midia, que insiste em entrevista-los como uma especie de "tecno-rebeldes". Recusaram uma aparicao na MTV exatamente p. prevenir este tipo de enfoque. Eles tem que preservar a imagem atual, de que "hacking" pode ser mais uma ajuda do que uma ameaca para a sociedade. Eles tem uma pagina WWW, se nao me engano no URL http://www.artcom.de/ccc.
Entre outras coisas, o CCC e' um clube voltado para o avanco do trafico de

dados. Antes da Internet se tornar uma possibilidade ate' mesmos uma possibilidade para a maioria, eles ja' trabalhavam em intercomunicacao de BBSES, como forma de ligar grupos pacifistas e em defesa do verde, coisa que hoje e' conhecida como Greennet. Isso foi durante a guerra do golfo. Mais que um club de hacking, era uma forma de difundir uma tecnologia improvisada, que hoje e' o "ultimo grito da moda". Os modens eram feitos por estudantes de eletronica. Jens, por exemplo: Durante a guerra ele ouviu noticias sobre uma BBS onde alguns ativistas se encontravam. Ficou interessado e comprou seu primeiro modem, para discutir com o grupo formas de melhorar o mundo.

Quando a guerra na ex-Yugoslavia comecou um grupo viajou para la' para la' e a ideia era colocar os ativistas em contato atraves de correio eletronico. So' que para isso seria necessario instalar BBSes e elas teriam dificuldades para se comunicar umas com as outras. Ficou estabelecido entao que o grupo faria ligacoes interurbanas de Bielefeld para cada uma das BBSes para garantir o contato entre elas. Esta sendo montada agora uma em Sarajevo, mas esbarra edificuldades como falta de eletricidade e o fato de que as pessoas nao compreendem, acham que existem coisas mais importantes do que fazer teleconferencia no meio de bomba caindo. Mas os resultados estao aparecendo, sob forma de ajuda as equipes de socorro e apoio, que sao organizadas desta forma, alem de ajudar na busca de parentes separados pelo combate. Vale lembrar que nao existe comunicacao telefonica entre a Servia e a Croacia, e esse e' tambem um meio de organizar as equipes de ajuda, de primeiros socorros e colocar grupos pacifistas em contato.

Parte desse esforco esta' detalhado no "Zagreb Diary" de Wam Kat. Ele dirigia um BBS em Zagreb, e durante tres anos a cada numero de dias enviava trechos descrevendo sua luta para manter o network funcionando. Uma amiga minha me informou que o sistema de comunicacao ficou tao bom que o pessoal em luta resolveu acabar com ele. Nao tive muitos detalhes e ainda nao cheguei no final do diario p. saber. Mas pela leitura do primeiro ano, nao so' foi um sucesso, mas que se manteve em pe' apesar das bombas e do resto.

Nem todo mundo esta' voltado para o lado tecnico de hacking, nessas horas, alguns veem isso mais como uma forma de ajudar o proximo, um passo em direcao a um mundo sem diferencas etnicas. A Alemanha esteve durante muito tempo dividida e esses jovens do CCC de Bielefeld estao voltados para ajudar Servios e Croatas senao a acabar, pelo menos aliviar ou diminuir os sofrimentos causados pela guerra.

(OBS: Este artigo e' meio datado. Comecei a produzi-lo durante agosto e setembro. Com os ultimos acontecimentos, a parte da guerra na ex-Yugoslavia perdeu um pouco a atualidade, ja' que pode a paz finalmente pode ter chegado)

HACKING CHIPS ON CELLULAR PHONES IS THE LATEST THING IN THE DIGITAL UNDERGROUND

by John Markoff

In Silicon Valley, each new technology gives rise to a new generation of hackers. Consider the cellular telephone. The land-based telephone system was originally the playground for a small group of hardy adventurers who believed mastery of telephone technology was an end in itself. Free phone calls weren't the goal of the first phone phreaks. The challenge was to understand the system.

The philosophy of these phone hackers: Push the machines as far as they would go.

Little has changed. Meet V.T. and N.M., the nation's most clever cellular phone phreaks. (Names here are obscured because, as with many hackers, V.T. and N.M.'s deeds inhabit a legal gray area.) The original phone phreaks thought of themselves as "telecommunications hobbyists" who explored the nooks and crannies of the nation's telephone network - not for profit, but for intellectual challenge. For a new generation of mobile phone hackers, the cellular revolution offers rich new veins to mine.

V.T. is a young scientist at a prestigious government laboratory. He has long hair and his choice in garb frequently tends toward Patagonia. He is generally regarded as a computer hacker with few equals. N.M. is a self-taught hacker who lives and works in Silicon Valley. He has mastered the intricacies of Unix and DOS. Unusually persistent, he spent almost an entire year picking apart his cellular phone just to see how it works.

What V.T. and N.M. discovered last year is that cellular phones are really just computers - network terminals - linked together by a gigantic cellular network. They also realized that just like other computers, cellular phones are programmable.

Programmable! In a hacker's mind that means there is no reason to limit a cellular phone to the paltry choice of functions offered by its manufacturer. That means that cellular phones can be hacked! They can be dissected and disassembled and put back together in remarkable new ways. Optimized!

Cellular phones aren't the first consumer appliances to be cracked open and augmented in ways their designers never conceived. Cars, for example, are no longer the sole province of mechanics. This is the information age: Modern automobiles have dozens of tiny microprocessors. Each one is a computer; each one can be reprogrammed. Hot rodding cars today doesn't mean throwing in a new carburetor; it means rewriting the software governing the car's fuel injection system.

This is the reality science fiction writers William Gibson and Bruce Sterling had in mind when they created cyberpunk: Any technology, no matter how advanced, almost immediately falls to the level of the street. Here in Silicon Valley, there are hundreds of others like V.T. and N. M. who squeeze into the crannies of any new technology, bending it to new and more exotic uses.

On a recent afternoon, V.T. sits at a conference room table in a San Francisco highrise. In his hand is an OKI 900 cellular phone. It nestles comfortably in his palm as his fingers dance across the keyboard. Suddenly, the tiny back-lit screen flashes a message: "Good Timing!"

Good Timing? This is a whimsical welcome message left hidden in the phone's software by the manufacturer's programmers. V.T. has entered the phone's software sub-basement - a command area normally reserved for technicians. This is where the phone can be reprogrammed; a control point from which the phone can be directed to do new and cooler things. It is hidden by a simple undocumented password.

How did V.T. get the password, or even know one was required? It didn't even take sophisticated social engineering - the phone phreak's term for gaining secret engineering data by fooling unwitting employees into thinking they are talking to an official phone company technician.

Rather, all he did was order the technical manual, which told him he needed special codes to enter the software basement. V.T. then called the cellular phone maker's technical support hotline. "They said 'sorry about that,' and asked for a fax number.

A couple of minutes later we had the codes," he recalls with a faint grin.

V.T.'s fingers continue darting across the keys - he is issuing commands built into the phone by the original programmers. These commands are not found in the phone's user manual. Suddenly, voices emerge from the phone's ear piece. The first is that of a salesman getting his messages >from a voice mail system. V.T. shifts frequencies. Another voice. A woman giving her boss directions to his next appointment.

What's going on here? V.T. and N.M. have discovered that every cellular phone possesses a secret mode that turns it into a powerful cellular scanner.

That's just the beginning. Using a special program called a "disassembler," V.T. has read-out the OKI's software, revealing more than 90 secret commands for controlling the phone.

That's how the two hackers found the undocumented features that turn the phone into a scanner. Best of all, the manufacturer has included a simple interface that makes it possible to control the phone with a standard personal computer.

A personal computer! The most programmable of a hacker's tools! That means that what appears to be a simple telephone can be easily transformed into a powerful machine that can do things its designers never dreamed of!

V.T. and N.M. have also discovered that the OKI's 64-Kbyte ROM - a standard off-the-shelf chip that stores the phone's software - has more than 20 Kbytes of free space. Plenty of room to add special features, just like hot rodding the electronics of a late-model car. Not only do the hackers use the software that is already there, but they can add some of their own as well. And for a good programmer, 20 Kbytes is a lot of room to work with.

It is worth noting that V.T. and N.M. are not interested in getting free phone calls. There are dozens of other ways to accomplish that, as an anonymous young pirate recently demonstrated by stealing the electronic serial number from a San Diego roadside emergency box and then racking up thousands of phone calls before the scam was discovered. (Such a serial number allowed the clever hacker to create a phone that the phone network thought was somewhere on a pole by the side of the freeway.)

It's also possible to wander to street corners in any borough in New York City and find a code dude - street slang for someone who illegally pirates telephone codes - who will give you 15 minutes of phone time to any corner of the world for $10. These "dudes" find illegally gathered charge card numbers and then resell them on the street until telephone security catches on. The tip-off: often an unusually large number of calls to Ecuador or France emmanating from one particular street corner.

Then again, it's possible for you to join the code hackers who write telephone software that automatically finds codes to be stolen. Or you can buy a hot ROM - one that contains magic security information

identifying you as a paying customer. Either way, your actions would be untraceable by the phone company's interwoven security databases.

But free phone calls are not what V.T. and N.M. are about. "It's so boring," says V.T. "If you're going to do something illegal, you might as well do something interesting."

So what's tempting? N.M. has hooked his portable PC and his cellular phone together. He watches the laptop's screen, which is drawing a map of each cellular phone call currently being placed in our cell - a term for the area covered by one broadcast unit in the cellular phone network. The network can easily query each cellular phone as to its current location. When phones travel from one cell to the next - as they tend to do in a car - information is passed on in the form of hidden code married to the phone transmission. Since N.M. knows where each local cell is, he can display the approximate geographic locations of each phone that is currently active.

But for that tracking scheme to work, the user must be on the phone. it would take only a few days of hacking to extend the software on N.M.'s PC to do an even more intriguing monitoring task: Why not pirate the data from the cellular network's paging channel (a special frequency that cellular networks use to communicate administrative information to cellular phones) and use it to follow car phones through the networks? Each time there is a hand-off from one cell to the next, that fact could be recorded on the screen of the PC - making it possible to track users regardless of whether or not they are on the phone.

Of course this is highly illegal, but N.M. muses that the capability is something that might be extremely valuable to law enforcement agencies - and all at a cost far below the exotic systems they now use.

Hooking a cellular phone to a personal computer offers other surveillance possibilities as well. V.T. and N.M. have considered writing software to monitor particular phone numbers. They could easily design a program that turns the OKI 900 on when calls are originated >from a specific number, or when specific numbers are called. A simple voice-activated recorder could then tape the call. And, of course, a reprogrammed phone could automatically decode touch-tone passwords - making it easy to steal credit card numbers and voice-mail codes.

Then there's the vampire phone. Why not, suggests V.T., take advantage of a cellular phone's radio frequency leakage - inevitable low-power radio emissions - to build a phone that, with the press of a few buttons, could scan the RF spectrum for the victim's electronic serial number. You'd have to be pretty close to the target phone to pick up the RF, but once you have the identity codes, a reprogrammed phone becomes digitally indistinguishable from the original. This is the type of phone fraud that keeps federal investigators up at night.

Or how about the ultimate hacker's spoof? V.T. has carefully studied phone company billing procedures and found many examples of inaccurate bills. Why not monitor somebody's calls and then anonymously send the person a corrected version of their bill: "According to our records...."

Of course, such software hacks are probably highly illegal, and authorities seem to be catching on. The Electronic Communi-cations Privacy Act of 1986 makes it a federal crime to eavesdrop on cellular phone calls. More recently, Congress passed another law forbidding the manufacture of cellular scanners. While they may not be manufacturers,

both N.M. and V.T. realize that their beautifully crafted phones are probably illegal.

For now, their goals are more modest. V.T., for example, would like to be able to have several phones with the same phone number. Not a problem, as it turns out. Although federal law requires that electronic serial numbers be hidden in specially protected memory locations, V.T. and N.M. have figured out how to pry the OKI's ESN out and write software so that they can replace it with their own number.

V.T. and N.M.'s explorations into the soul of the OKI 900 have left them with a great deal of admiration for OKI's programmers. "I don't know what they were thinking, but they had a good time," V.T. said, "This phone was clearly built by hackers."

The one thing V.T. and N.M. haven't decided is whether or not they should tell OKI about the bugs - and the possibilities - they've found in the phone's software.===

E' talvez o primeiro documentario serio sobre a comunidade hacker. O unico defeito e' a duracao do mesmo. So' trinta minutos. Recebeu otimas criticas das autoridades no assunto. Nao tinha nem como nao receber esses elogios: Mais da metade estao no filme. Nele e' possivel se tomar contato com a maioria dos expoentes da cultura. Como por exemplo, conhecer a familia de um menino de 13 anos, que recebeu a visita do servico secreto americano, e sua versao para o fato de ter conseguido escapar a prisao.
("Definitivamente minha idade. Tinha o fato de que eu so' queria o acesso, nao os dados, nao destrui nada. Minha idade, definitivamente minha idade .. pegava mal mandar prender um garoto de 13 anos por acusacao de espionagem..por essa e outras eles resolveram suspender as acusacoes..")
Muito legal ver os pais explicando o que pensavam do filho ter invadido o sistema responsavel, entre outras coisas, pela fabricacao de ogivas nucleares.

Outro lance interessante sao cenas mostrando acessos ilegais e coisas do genero, inclusive algo do qual nao ouvia falar ha tempos: Trashing. Isso e' basicamente vasculhar lixo de grandes empresas em busca de codigos ou numeros de telefones, senhas e coisas do genero. Merece destaque tambem os hackers com imunidade para haquear, pois tem a funcao de dedurar colegas que se dediquem a invasao de sistemas. Do lado europeu, fotos e depoimentos do Congresso de Hackers na Holanda. O Caos Computer Club tambem aparece, e fala de uma parte da atividade hacker que nao aparece muito na imprensa: a criacao de um network para ajudar os grupos de ajuda na Iugoslavia assolada pela guerra, ou como alta tecnologia pode ser usada para ajudar de formas que ninguem pensaria.
Tem muito sobre o o que e o porque da atividade hacking, mas nao o como. De qualquer forma, trata-se de algo bem mais realista do que qualquer coisa nos jornais, revistas ou televisao. Existe um URL dedicado ao documentario, no http://www.bianca.com/bump/ua.html, onde tambem tem informacoes sobre como conseguir o dito.

UNAUTHORIZED ACCESS - O DOCUMENTARIO

E' talvez o primeiro documentario serio sobre a comunidade hacker. O unico defeito e' a duracao do mesmo. So' trinta minutos. Recebeu otimas criticas das autoridades no assunto. Nao tinha nem como nao receber esses elogios: Mais da metade estao no filme. Nele e' possivel se tomar contato com a maioria dos expoentes da cultura. Como por exemplo, conhecer a familia de um menino de 13 anos, que recebeu a visita do servico secreto americano, e sua versao para o fato de ter conseguido escapar a prisao.
("Definitivamente minha idade. Tinha o fato de que eu so' queria o acesso, nao os dados, nao destrui nada. Minha idade, definitivamente minha idade .. pegava mal mandar prender um garoto de 13 anos por acusacao de espionagem..por essa e outras eles resolveram suspender as acusacoes..")
Muito legal ver os pais explicando o que pensavam do filho ter invadido o sistema responsavel, entre outras coisas, pela fabricacao de ogivas nucleares.

Outro lance interessante sao cenas mostrando acessos ilegais e coisas do genero, inclusive algo do qual nao ouvia falar ha tempos: Trashing. Isso e' basicamente vasculhar lixo de grandes empresas em busca de codigos ou numeros de telefones, senhas e coisas do genero. Merece destaque tambem os hackers com imunidade para haquear, pois tem a funcao de dedurar colegas que se dediquem a invasao de sistemas. Do lado europeu, fotos e depoimentos do Congresso de Hackers na Holanda. O Caos Computer Club tambem aparece, e fala de uma parte da atividade hacker que nao aparece muito na imprensa: a criacao de um network para ajudar os grupos de ajuda na Iugoslavia assolada pela guerra, ou como alta tecnologia pode ser usada para ajudar de formas que ninguem pensaria.

Tem muito sobre o o que e o porque da atividade hacking, mas nao o como. De qualquer forma, trata-se de algo bem mais realista do que qualquer coisa nos jornais, revistas ou televisao. Existe um URL dedicado ao documentario, no http://www.bianca.com/bump/ua.html, onde tambem tem informacoes sobre como conseguir o dito.

THE BULGARIAN AND SOVIET VIRUS FACTORIES

Vesselin Bontchev, Director
Laboratory of Computer Virology
Bulgarian Academy of Sciences, Sofia, Bulgaria

0) Abstract

It is now well known that Bulgaria is leader in computer virus production and the USSR is following closely. This paper tries to answer the main questions: Who makes viruses there, What viruses are made, and Why this is done. It also underlines the impact of this process on the West, as well as on the national software industry.

1) How the story began

Just three years ago there were no computer viruses in Bulgaria. After all, these were things that can happen only in the capitalist countries. They were first mentioned in the April issue of the Bulgarian computer magazine "Komputar za vas" ("Computer for you") [KV88] in a paper, translated from the German magazine "Chip" [Chip]. Soon after that, the same Bulgarian magazine published an article [KV89]], explaining why computer viruses cannot be dangerous. The arguments presented were, in general, correct, but the author had completely missed the fact that the majority of PC users are not experienced programmers.

A few months later, in the fall of the same year, two men came in the editor's office of the magazine and claimed that they have found a computer virus. Careful examination showed that it was the VIENNA virus.

At that time the computer virus was a completely new idea for us. To make a computer program, whose performance resembles a live being, is able to replicate and to move from computer to computer even against the will of the user, seemed extremely exciting.

The fact that "it can be done" and that even "it had been done" spread in our country like wildfire. Soon hackers obtained a copy of the virus and began to hack it. It was noticed that the program contains no "black magic" and that it was even quite sloppily written. Soon new, home--made and improved versions appeared. Some of them were produced just by assembling the disassembly of the virus using a better optimizing assembler. Some were optimized by hand. As a result, now there are several versions of this virus, that were created in Bulgaria --- versions with infective lengths of 627, 623, 622, 435, 367, 353 and even 348 bytes. The virus has been made almost two times shorter (its original infective length is 648 bytes) without any loss of functionality.

This virus was the first case. Soon after that, we were "visited" by the CASCADE and the PING PONG viruses. The later was the first boot--sector virus and proved that this special area, present on every diskette can be used as a virus carrier, too. All these three viruses were probably imported with illegal copies of pirated programs.

2) Who, What & Why.

2.1) The first Bulgarian virus.

At that time both known viruses that infected files (VIENNA and CASCADE) infected only COM files. This made me believe that the infection of EXE files was much more difficult. Unfortunately, I made the mistake by telling my opinion to a friend of mine. Let's call him "V.B." for privacy reasons.(1)
[(1) These are the initials of his true name. It will be the same with the other virus writers that I shall mention. Please note, that while I have the same initials (and even his full name resembles mine), we are two different persons.]
The challenge was taken immediately and soon after that I received a simple virus that was able to infect only EXE files. It is now known to the world under the name of OLD YANKEE. The reason for this is that when the virus infects a new file, it plays the "Yankee Doodle" melody.

The virus itself was quite trivial. Its only feature was its ability to infect EXE files. The author of this virus even distributed its source code (or, more exactly, the source code of the program that releases it). Nevertheless, the virus did not spread very widely and even had not been modified a lot. Only a few sites reported to be infected by it. Probably the reason for this was the fact, that the virus was non--resident and that it infected files only on the current drive. So the only possibility to get infected by it was to copy an infected file from one computer to another.

When the puzzle of creating a virus which is able to infect EXE files was solved, V.B. lost his interest in this field and didn't write any other viruses. As far as I know, he currently works in real--time signal processing.

2.2) The T.P. case.

The second Bulgarian virus--writer, T.P., caused much more trouble. When he first heard the idea about aself--replicating program, he was very interested, decided to writehis own virus, and he succeeded. Then he tried to implement a virus protection scheme and succeeded again. The next move was to improve his virus to bypass his own virus protection, then to improve the virus protection and so on. That is why there are currently about 50 different versions of his viruses.

Unfortunately, several of them (about a dozen) were quite "successful." They spread world--wide. There are reports about them from all countries of the former Eastern block, as well as from the USA and West Europe.

Earlier versions of these TP viruses are known under the name VACSINA, because they contain such a string. In fact, this is the name of the virus author's virus protection program. It is implemented as a device driver with this name. The virus merely tries to open a file with this name, which means "Hey, it's me, let me pass."

The latest versions of the virus are best known under the name YANKEE DOODLE, because they play this tune. The conditions on which the tune is played are different with the different versions of the virus --- for instance when the user tries to reboot the system, or when the system timer reaches 5 p.m.

All TP viruses are strictly non--destructive. Their author payed particular attention not to destroy any data. For instance, the virus does not infect EXE files for which the true file length and the length of the loadable part as it is present in the EXE header, are not equal. As far as I know, no other virus that is able to infect EXE files works this way.

Also, the virus does not try to bypass the resident programs that have intercepted INT 13h, therefore it takes the risk to be detected by most virus activities monitoring software. The author of the virus obviously could circumvent it --- for instance it uses a clever technique, now known as "interrupt tracing" to bypass all programs that have hooked INT 21h. The only reason for not bypassing INT 13h as well, is that this would also bypass all disk casheing programs, thus it could cause damage.

Of course, the fact that the virus is not intentionally destructive does not mean that it does not cause any damage. There are several reports of incompatibilities with other software; or of panicking users, that have formatted their disks; or, at least, damage caused by time loss, denial of computer services, or expenses removing the virus. It is well known, that "there ain't no such thing as a good virus."

The TP viruses were not spread intentionally; the cause could be called "criminal negligence." The computer used by T.P. to develope his viruses was also shared by several other people. This is common practice in Bulgaria, where not everyone can have a really "personal" computer to work with. T.P. warned the other users that he is writing viruses, but at this time computer viruses were a completely new idea, so nobody took the warning seriously. Since T.P. didn't bother to clean up after himself, these users got, of course, infected. Unintentionally, they spread the infection further.

When asked about the reason of writing viruses, T.P. replied that he did this in order to try several new ideas; to better learn the operating system and several programming tricks. He is not interested in this field any more --- he has stopped writing viruses about two years ago.

2.3) The Dark Avenger.

In the spring of 1989 a new virus appeared in Bulgaria. It was obviously "home--made" and just to remove any doubts about it, there was a string in it, saying "This program was written in the city of Sofia (C) 1988-89 Dark Avenger."

The virus was incredibly infectious --- when it was in memory, it was sufficient to copy or just to open a file to get it infected. When the user felt that there is a virus in his/her system and, without booting from a non--infected write--protected system diskette, ran an anti--virus program which wasn't aware of this new virus, he usually got all his/her executable files infected.

The idea of infecting a file when it is opened was new and really "successful." Now such viruses are called "fast infectors." This strategy helped the virus to spread world-- wide. There are reports from all European countries, from the USA, the USSR, even from Thailand and Mongolia.

On the top of this, the virus was very dangerously destructive. On each 16th run of an infected program, it overwrote a sector on a random place of the disk, thus possibly destroying the file or directory that contained this sector. The contents of the overwritten sector was the first 512 bytes of the virus body, so even after the system has been cleaned up, there were files, containing a string "Eddie lives...somewhere in time!" This was causing much more damage than if the virus was just formatting the hard disk, since the destruction was very unnoticable and when the user eventually discovered it, his backups probably already contained corrupted data.

Soon after that, other clever viruses began to appear. Almost all of them were very destructive. Several contained completely new ideas. Now this person (we still cannot identify him exactly) is believed to be the author of the following viruses:

DARK AVENGER, V2000 (two variants), V2100 (two variants), 651, DIAMOND (two variants), NOMENKLATURA, 512 (six variants), 800, 1226, PROUD, EVIL, PHOENIX, ANTHRAX, LEECH...

Dark Avenger has several times attacked some anti--virus researchers personally. The V2000/V2100 viruses claim to be written by "Vesselin Bontchev" and in fact hang the computer when any program, containing this string is run. A slightly modified variant of V2100 (V2100-B) has been used to trojanize version 66 of John McAfee's package VIRUSCAN.

There are reports that Dark Avenger has called several bulletin board systems in Europe and has uploaded there viruses. The reports come from the UK, Sweden, the Netherlands, Greece... Sometimes the viruses uploaded there are unknown in Bulgaria (NOMENKLATURA,ANTHRAX). But they are obviously made in our country --- they contain messages in Cyrillic. Sometimes Dark Avenger uploads a Trojan program that spreads the virus --- not just an infected program. This makes the detection of the source of infection more difficult.

One particular case is when he has uploaded a file called UScan, which, when run, claims to be the "universal virus scanner," written by Vesselin Bontchev. Even the person who has uploaded it, has logged under the name "Vesselin Bontchev." In fact, the program just infected all scanned files with the ANTHRAX virus.

While the other Bulgarian virus writers seem to be just irresponsible or with childish mentality, the Dark Avenger can be classified as a "technopath." He is a regular user of several Bulgarian bulletin

board systems, so one can easily exchange e-mail messages with him. When asked why his viruses are destructive, he replied that "destroying data is a pleasure" and that he "just loves to destroy other people's work."

Unfortunately, no measures can be taken against him in Bulgaria. Since there is no law for information protection, his activities are not illegal there. He can be easily caught by tapping the phones of the BBSes that he uses, but the law enforcement authorities cannot take such measures, since there is no evidence of illegal activities. Alas, he knows this perfectly.

2.4) Lubo & Ian.

Some of the Dark Avenger's viruses proved to be very "successful" and caused real epidemics. That is why they were often imitated by other virus writers, that had no imagination to design their own virus, but were jealous of Dark Avenger's fame. So they just disassembled his viruses (usually the first one) and used parts of it --- sometimes without even understanding their purpose. Such is the case with the MURPHY viruses.

According to a string in them, they are written by "Lubo & Ian, USM Laboratory, Sofia." These people do exist and they have used their real names. "Lubo" has even been several times interviewed by newspaper's reporters.

They claim that the virus was written for vengeance. They have done some important work for their boss and the latter refused to pay them. That is why they developed te virus in one night and released it. The fact that the virus will spread outside the laboratory just didn't come to their minds. However, this does not explain the developing of the other versions of the same virus (there are at least four variants). Nevertheless, it proves one more time that it is better (and safer, too) to pay the good programmers well...

Besides MURPHY, these two virus writers have created another virus, called SENTINEL (5 variants). The only unusual thing with this virus is that it is written in a high--level programming language (Turbo PASCAL), but is not an overwriting or a companion virus as most HLL viruses are. It is able to infect COM and EXE files by appending itself to them and by preserving their full functionality. It is also memory resident, hides the file length increase when the user issues the DIR command, and even mutates.

2.5) The virus writer from Plovdiv.

This man, P.D., claimed that he has written viruses "for fun" and only "for himself" and that he "never releases them." Unfortunately, at least two of them have "escaped" by accident. These are the ANTI-PASCAL605 and the TERROR viruses. Especially the latter is extremely virulent and caused a large epidemic in Bulgaria.

P.D. was very sorry for that and submitted examples of all his viruses to the anti--virus researchers so that the respective anti--virus programs be developed --- just in case some of these viruses escapes too. These viruses turned out to be quite a few, ranging from extremely stupid to very sophisticated. Here are some of

them:

XBOOT, ANTIPASCAL (5 variants), TINY (11 variants), MINIMAL-45, TERROR, DARK LORD, NINA, GERGANA, HAPPY NEW YEAR (2 variants), INT 13.

P.D. claims that the DARK LORD virus (a minor TERROR variant) is not written by him. The TINY family has nothing to do with the Danish TINY virus (the 163--byte variant of the KENNEDY virus), and, as well as the MINIMAL-45 virus, are written with the only purpose to make the shortest virus in the world.

Now P.D. is not writing viruses any more --- because "it is so easy, that it is not interesting," according to his own words. He is currently writing anti--virus programs --- and rather good ones.

2.6) The two guys from Varna.

They are two pupils (V.P. and S.K.) from the Mathematical High School in Varna (a town on the Black Sea). They have developed several viruses and continue to do so, producing more and more sophisticated ones. Furthermore, they intentionally spread their viruses, usually releasing them on the school's computers or in the Technical University in Varna. When asked why they write and release viruses, they reply "because it's so interesting!"

The viruses written by them are: MG (5 variants), SHAKE (5 variants), DIR and DIR II. All of them are memory resident and infect files when the DIR command is performed.

The last one is an extremely virulent and sophisticated virus --- as sophisticated, as THE NUMBER OF THE BEAST. It is also a completely new type of virus --- it infects nether boot sectors, nor files. Instead, it infects the file system as a whole, changing the information in the directory entries, so that each file seems to begin with the virus.

There is a counter of the number of infected systems in the virus body. There is evidence that V.P. and S.K. collect infected files, copy the contents of the counter and then draw curves of the spread of infection, checking the normal distribution law. They are doing this "for fun."

2.7) W.T.'s case.

W.T. is a virus writer from Sofia, who has written two viruses --- WWT (2 variants) and DARTH VADER (4 variants). According to his own words, he has done so to test a new idea and to gain access to the Virus eXchange BBS (see below).

The new idea consisted of a virus (DARTH VADER) that does not increase file lengths, because it searches for unused holes, filled with zeros, and writes itself there. Also, the virus does not perform any write operations. Instead, it just waits for a COM file to be written to by DOS and modifies the file's image in memory just before the write operation is performed.

W.T. does not write viruses any more, but he is still extremely

interested in this field. He is collecting sophisticated viruses and disassembles them, looking for clever ideas.

2.8) The Naughty Hacker.

This virus writer, M.H., is a pupil and also lives in Sofia. He has written several viruses, most of which contain the string "Naughty Hacker" in their body. All of them are non-- destructive, but contain different video effects --- from display desynchronization to a bouncing ball.

Currently, at least 8 different variants are isolated, but it is believed that even more exist and are spread in the wild. Also, it is believed that M.H. continues to produce viruses. As usual, he is doing so "because it is interesting" and "for fun."

He is also the author of three simple boot sector viruses (BOOTHORSE and two others that are still unnamed).

2.9) Other known virus writers.

The persons listed above are the major Bulgarian virus producers. However, they are not alone. Several other people in Bulgaria have written at least one virus (sometimes more). In fact, making a virus is currently considered there a kind of sport, or a practical joke, or means of self--establishment.

Some of these virus writers have supplied their creations directly to the anti--virus researchers, as if they are waiting for a reward. This happens quite often --- probably they expect that the anti--virus researcher, as the best qualified person, will evaluate their creation better. Sometimes the fact that their virus becomes known, is described, and is included in the best anti--virus programs is sufficient for these people and they don't bother to really spread their virus in the wild. So, probably the main reason for these people to produce viruses is the seek of glory, fame, and self--establishment.

Such known Bulgarian virus writers (with the respective names of their viruses given in parentheses) are V.D. from Pleven (MICRO-128), A.S. and R.D. from Mihajlovgrad (V123), I.D. from Trojan (MUTANT, V127, V270x), K.D. from Tutrakan (BOYS, WARRIER, WARRIOR, DREAM), and others.

2.10) Unknown Bulgarian virus writers.

Of course, there are also other virus writers, that are not known to the author of this paper. Sometimes it is possible to determine the town where the viruses were developed --- usually due to an appropriate string in the virus body, or because the virus wasn't found elsewhere. Some of the viruses are very simple, others are quite sophisticated. Here are examples of such viruses.

- The KAMIKAZE virus has been detected only in the Institute of Mathematics at the Bulgarian Academy of Sciences, Sofia and is probably made there;

- The RAT virus, made in Sofia, as it is written in its body;

- The VFSI (HAPPY DAY) virus has been developed in the Higher Institute of Finances and Economics in Svishtov (a small town on the Danube) by an unknown programmer;

- The DESTRUCTOR virus, probably made in Plovdiv, where it has been first detected;

- The PARITY virus, probably written in the Technical University, Sofia, since it has not been detected elsewhere;

- The TONY file and boot sector viruses, probably created in Plovdiv where they have been first detected;

- The ETC virus, detected only in Sofia;

- The 1963 virus, a quite sophisticated one, probably made in the Sofia University;

- The JUSTICE virus.

2.11) The Virus eXchange BBS.

About a year ago, the virus writing in Bulgaria entered a new phase. The virus writers began to organize themselves. The first step was the creation of a specialized bulletin board system (BBS), dedicated to virus exchange. The Virus eXchange BBS.

It's system operator (SysOp), T.T. is a student of computer science in the Sofia University. He has established the BBS in his own home. On this BBS, there are two major kinds of files --- anti--virus programs and viruses. The anti--virus programs can be downloaded freely.

In order to get access to the virus area, one has to upload there a new virus. However, anyone who uploads a new virus, gets access to the whole virus collection. S/He could then download every virus that is already available, or even all of them. No questions are asked --- for instance for what reason s/he might need these viruses.

Furthermore, the SysOp takes no steps to verify the identity of his users. They are allowed to use fake names and are even encouraged to do so. Dark Avenger and W.T., between them are, the most active users, but there are also names like George Bush from New York, Saddam Hussein from Baghdad, Ozzy Ozburn and others.

Since this BBS has already a large collection of computer viruses (about 300), it is quite difficult to find a new virus for it. If one wants badly to get access to the virus area, it is much simpler to write a new virus, instead of trying to find a new one. That is exactly what W.T. did. Therefore, this BBS encourages virus writing.

Furthermore, on this BBS there are all kinds of viruses --- some of them as 1260, V2P6Z, FLIP, WHALE are considered as extremely dangerous, since they are using several new ideas and clever tricks, which makes them very difficult to be recognized and removed from the infected files. And the Virus eXchange BBS policy makes all these

viruses freely available to any hacker that bothers to download them. This will, undoubtedly, lead to the creation of more and more such "difficult" viruses in the near future.

The free availability of live viruses has already given its bitter fruits. It helped to viruses created far away from Bulgaria and not widely spread, to cause epidemics in our country. Such was the case of the DATALOCK virus. It has been created in California, USA and uploaded to the Virus eXchange BBS. A few weeks later it was detected in the Technical University, Sofia. Probably one of the users of the BBS had downloaded it from there and spread it "for fun." In the similar way the INTERNAL, TYPO and 1575 viruses entered our country.

But the free availability of known live viruses is not the most dangerous thing. After all, since they are already known, there already exist programs to detect and probably to remove them. Much more dangerous is the free availability on this BBS of virus source code! Indeed, original source code or well commented virus disassemblies of several viruses are freely available on the Virus eXchange BBS --- just as any other live virus. To name a few, there are:

DARK AVENGER, OLD YANKEE, DIAMOND, AMSTRAD, HYMN, MLTI830, MURPHY, MAGNITOGORSK, ICELANDIC, MIX1, STONED, JERUSALEM, DATACRIME, BURGER, ARMAGEDON, OROPAX, DARTH VADER, NAUGHTY HACKER, 512, VIENNA, 4096, FISH#6, PING PONG, BLACK JEC, WWT, MG, TSD, BOOTHORSE, BAD BOY, LEECH...

Most of them are perfectly assemblable sources.

The publishing of virus source code has proven to be the most dangerous thing in this field. The VIENNA, JERUSALEM, CASCADE and AMSTRAD viruses are the best examples. Their source code has been made publicly available, which led to the creation of scores of new variants of these viruses. The known variants of only these four viruses are about 20 % of all known viruses, which means more than a hundred variants. One can imagine the consequences of making publicly available the source code of all the viruses listed above. In less than a year we probably will be submerged by thousands new variants...

In fact, this process has already begun. The HIV, MIGRAM, KAMASYA, CEMETERY and ANTICHRIST viruses have been obviously created by someone who had access to the source of the MURPHY virus. The ENIGMA virus is clearly based on the OLD YANKEE code. There have been reports about infections with these viruses in one Italian school and an Italian virus writer, known as Cracker Jack is a user of Virus eXchange...

The damage caused by this BBS alone to the rest of the world is big enough. But this is not all. Since possession of "viral knowledge" (i.e., live viruses, virus source code) has always tempted hackers and since the legitimate anti--virus researchers usually exchange such things only between themselves and in a very restricted manner, it is not surprising that similar "virus boards" began to pop up around the world. There are currently such BBSes in the USA, Germany, Italy, Sweden, Czechoslovakia, the UK and the Soviet Union. Stopping their activities is very difficult in legal terms, because the possession, storage or willful downloading of computer viruses usually is not considered as a criminal offence. And it shouldn't be

--- otherwise the anti--virus researchers themselves will not have a
way to exchange virus samples to work with.

The creation of a virus--oriented BBS, the system operator of which
supported the writing, spreading and exchanging of virus code didn't
go unnoticed in Bulgaria. Almost all virus writers have obtained a
modem (a not very easy thing in Bulgaria) and contacted it.
Afterwards, they began to contact each other by means of electronic
messages on this BBS. They have even created a specialized local
conference (local for Bulgaria), in order to keep in touch and to
exchange ideas how to write clever viruses. Therefore, they began to
organize themselves --- a thing that cannot be said about the
anti--virus research community in all countries...
{a continuar}
arquivo: bulgarian.factory.doc
Origem: info.cert.org   subdiretorio pub/virus-l/docs

CARTAS - DICAS

CARTAS

Subject: Oracao a "Sao Megabyte"

Bem, pessoal... essa apareceu numa lojinha na Rua Santa Ifigenia, em
Sao Paulo.

    Oracao a Sao Megabyte

File nosso que esta' no HD
Backupeados sejam vossos bytes
Venha ao DOS o vosso prompt
Seja feito o vosso restore assim em
Rede como em disco
O bit nosso de cada tecla gravai hoje
Atualizai os nossos arquivos
Assim como nos atualizamos os nossos equipamentos
Mas nao nos deixeis cair a rede e
Ativai-nos o poderoso no-break
Pois vossa e' a CPU e a memoria
Para todo o processamento
HIGH MEM

Subject: Re: Irc

submeta informatica-jb
On Mon, 20 Nov 1995, RICARDO Sant'Ana wrote:

> submeta informatica-jb
>
>   Ola
>
>   recentemente eu li algo sobre Irc aqui nesta lista e tenho uma duvida ...
> eu uso Unix, e realmente e' necessario um programa para eu me conectar Ircs ??
> Se nao, como eu faco para me conectar a um Irc...se eu nao me engano, Irc sao
> servidores que podem ser acessados via telnet, portanto, quais seriam os

endere
> cos ??
>
>   Obrigado, Spanish_eyes
>

Oi!

V nao precisa mesmo instalar o irc p/ v, por telnet eu sei que da certo,
mas nao me lembro mais como fazer, porque e' muito ruim!! O lag (demora
p/ vir as respostas) e' tao grande que fica impossivel conversar! Entao
eu acho que e' muito mais negocio v instalar um, principalmente porqeu ai
v pode usar uns scripts p/ fazer uns aliases! Quebra um galhao! V tb pode
entrar por bbs. Eu conheco duas aqui no brasil que tem esse servico. Uma
e' a jacare = telnet jacare.secom.ufpa.br, e a outra e' a ururau =
bbs.uenf.br. Mas tb e' bem lento!!!

T+

Subject: Re: Irc - qual o login ???

submeta informatica-jb
On Thu, 23 Nov 1995 ????????@????.???.br wrote:
> > v pode usar uns scripts p/ fazer uns aliases! Quebra um galhao! V tb pode
> > entrar por bbs. Eu conheco duas aqui no brasil que tem esse servico. Uma
> > e' a jacare = telnet jacare.secom.ufpa.br, e a outra e' a ururau =
> > bbs.uenf.br. Mas tb e' bem lento!!!
>
> Eu li sua mensagem na lista e me interessei so que voce esqueceu de dizer
> qual o login e a passwd, please mande-os 8-).
>

Oi!

Desculpa por ter esquecido, ai vai:
bbs.uenf.br --> login: bbs
nao pede password, e vem as instrucoes na tela p/ se cadastrar (nao paga
nada), ai e'so colocar os seus dados, nome, e-mail, username, a sua
password, etc.

jacare.secom.ufpa.br --> login: bbs
password: bbs
o resto e'igual ao da uenf!

Eu tb achei alguns enderecos p/ acessar via telnet:
telnet sci.dixie.edu (6677) ou(7766)
telnet skywarrior.ecn.uoknor.edu (6677)
telnet intruder.ecn.uoknor.edu (6677)
telnet skyraider.ecn.uoknor.edu (6677)
telnet wildcat.ecn.uoknor.edu (6677)
T+
{Nome e email editados}

OBSERVACAO: A pagina http://www.tucows.com tem uma lista de programas muito
interessantes, inclusive o mIRC, facilimo de instalar e otimo p. IRC. Para
quem nao quiser suar lendo o manual, os unicos comandos realmente importan-
tes sao:

/list
/join

ex: /join brasil

/part

ex: /part brasil

/help

Usando o mIRC, o negocio e' instalar, teclar cntrl-e, escolher um SERVER (depois voce descobre o que e') prencher seus dados (quer ser quem? Bill Clinton? Michael Jackson?) e teclar Alt-c. Depois /list e /join .
No inicio, nao precisa falar, se nao quiser. O mundo do IRC permite cada coisa incrivel, inclusive a transferencia de arquivos.

From: Rafael Jorge Csura Szendrodi
Subject: Como desinfectar um computador contaminado

submeta virus, informatica-jb

Ola pessoal,

Venho por esta dar algumas dicas de como proceder a descontaminacao de um computador contaminado por virus.

1 - Tenha sempre a mao um disquete de boot e um disquete com um antivirus, todos os dois PROTEGIDOS PARA A ESCRITA, somente assim se evitara eles sejam contaminados acidentalmente.

2 - Ligue o computador e sete na BIOS para ele dar boot primeiro pelo drive A, somente assim se tera garantia de que o virus nao ira se instalar na memoria do computador.

3 - Apos o boot, insira o disquete com antivirus e carregue o mesmo no computador. Como primeira acao, recomendo que voce escaneie uma vez somente para reportar a existencia de virus, assim se sabera quais os arquivos contaminados e quais as providencias a tomar.

4 - Apos anotar ou imprimir os nomes dos arquivos, sete a acao para desinfeccao automatica, e volte a escanear o computador. Porem alguns virus como o FREDDY KRUEGER nao sao passiveis de desinfeccao, ai o jeito e deletar os arquivos (AUTOMATIC DELETION).

5 - Se nao houver mensagens reportando virus, entao tente usar seu computador normalmente, se voltar a ocorrer problemas, suspeite de um virus novo (UM VIRUS NOVO NAO E INDENTIFICAVEL PELOS ANTIVIRUS, A NAO SER QUE ELE SEJA UMA VARIANTE DE UM VIRUS CONHECIDO) e ai o jeito mesmo e FORMATAR O HD E TODOS OS DISQUETES QUE TENHAM PASSADO PELO COMPUTADOR CONTAMINADO.

6 - Espero ter dado uma ajuda para os novatos em virus.

Subject: Nasce mais um B... na Internet

submeta virus, informatica-jb

Venho por esta protestar contra a invasao a minha vida particular por um dos assinantes desta lista, um palhaco b... que nem sei quem e pois nao se identificou, nem teve coragem suficiente para entrar em contato diretamente comigo.

O sujeito viu a minha assinatura eletronica que todos voces ja conhecem "VIRUS MAKER", que e o apelido que tenho aqui na minerva devido a um falso virus que fiz no Borland 7.0 para assustar os usuarios desta rede que teimam em nao escanear os disquetes que trazem para ca. Como a maioria dos assinantes das listas da unicamp tem QI (quociente de inteligencia) alto, viu que estava entre aspas e era so um apelido, a ameba, porem, que tem QI (quociente de ignorancia) alto, achou, ou quiz achar, que eu faco virus mesmo e desencavou, nao sei onde, os telefones do trabalho do meu pai e telefonou para ele, que nem estava mais la, mas em reunio de diretores do clube onde ele e filiado, nao sei como conseguiu o telefone de la, e falou que a policia poderia me prender por fazer virus, ou que eu ia ser processado, e outras M... do genero.

Sobre esse cretino, que nao e homem o suficiente para entrar em contato direto comigo, so tenho a dizer que e mesmo um palhaco B...,e se a carapuca servir, logo logo ele vai botar o chapeu de palhaco para fora, para todo mundo ver.

Aqui na rede minerva todos sabem que sou virus collector (colecionador de virus) e que coleciono virus apenas para fins de pesquisa (realmente me considero um virusmaniaco, pois sou gamado em descobrir como funcionam tais programas que parecem ate seres vivos, alguns chegam ate a ter caracteristicas mutantes como nos animais), porem nunca contaminei propositalmente as redes onde possuo conta, nem os disquestes de meus amigos, nem nada. Sou ate util a rede como uma das poucas pessoas, se nao a unica, que se da ao trabalho de escanear os HDs da rede todos os dias. Tenho inclusive testemunhas para provar isso.

Para terminar, tenho a dizer que nao e crime nem colecionar virus (desde que voce nao contamine os computadores das outras pessoas) nem se assinar com o apelido "VIRUS MAKER", portanto se algum cretino voltar a seu intrometer na minha vida particular ou na de meus parentes, que se prepare para responder NA JUSTICA por isso, ou seja, o palhaco vai ter que telefonar para o advogado dele tambem.

Agradeco desde ja a atencao dispensada pelos demais assinantes da esquina-das-listas (listas virus e informatica-jb).

Forte abraco - ??????

?????? ????? ????? ?????????
"VIRUS MAKER" - Virus Collector
Ranking atual: Makers = 0 -> Isto quer dizer de so
coleciono virus, nao os faco.
Virus ou variantes = 9
Codigos-fonte de virus = 27

COMENTARIO DO EDITOR:
Ja' vi esse filme antes. Toda a minha solidariedade ao individuo acima. Posso acrescentar que na legislacao atual, nao existe nada contra: colecionar virus de computador, fazer virus de computador, infectar computadores com virus de computador. So' que isso nao livra as pessoas que fazem isso de serem perseguidas. A "patrulha ideologica" e' uma constante aqui no Brasil. E' preciso tomar cuidado. Ja' escrevi sobre isso no Barata Eletrica. Lembrem-se sempre: na legislacao brasileira, cabe ao reu provar a inocencia. Se voce for preso, ha' chances que vao tentar te incriminar com

alguma coisa, so' para nao perder a moral. Paranoia de vez em quando e' bom.

---

submeta informatica-jb

> Alguem por acaso teria a lista de provedores de internet que saiu na
> Internet World brasileira de outubro??
> Ariadne
>

Oi, ???????!

A lista e' essa aqui:

Banco Rural - (011)64-4987
(021)533-3008

BBS Magic Operator - (071)533-4445
(071)351-1615

BBS Unikey - (021)571-7701

Celtec - (021)512-1144

Centroin - (021)556-1524

Conex - (051)226-4808

DGLNet - (0192)32-9696
(011)837-7163

Dialdata - (011)829-4731

Embratel - 07821278 (gratuito)

GSI/IBM - (011)545-3022
(0800)214646

Horizontes BBS - (031)286-3420
(031)286-2000 (dados)

Ibase - (021)286-4467

Inside (IIS) - (021)537-0028

Internet Now - (011)887-1319

Mandic - (011)870-0888

NutecNet - (051)800-2227 (gratuito)
(011)505-5728
(051)225-7311

RioLink - (021)268-0717

SohoNet/Origin - (011)547-2656

STI - (011)884-2446 (dados)

Unisys - (011)525-8199

Viatel - (011)533-4005

#-#-#-#-#-#-#-#-#-#-#-

Qualquer informacao adicional, mande um Mail p/ mim que eu respondo.

[]'s
{Nome e email do autor editados}

Subject: Barata Eletrica !!!

Cara.. DEMAIS !!! So esta palavra significa o que i o seu FANZINE !!!

P A R A B E N S !!!

[]'s...

????? ????
Ribeirao Preto, SP, Brazil

Subject: barata eletrica

Prezado Derneval
Cara eu gostei muito dos seis numeros do Barata que peguei na internet, por isso estou te mandando este mail implorando mais publicacoes, com este ou com qualquer nome que voce colocar, pois nao importando o nivel de envolvimento ou conhecimento de computadores, voce conseguiu publicar um retrato de cada um de nos.
Cordialmente ????????.

???????? ?????? ????????
IF - IBCCF UFRJ
Sistemas Complexos, CAOS

To: Derneval R R da Cunha
Subject: Re: your mail

Fala Mestre !!! HAU !!!!!

E como vao as coisas com o BE ?...E por falar em Dr.Byte e zines...valeu o artigo...!!!

Realmente...precisamos nos reunir e definir alumas coisas...O que for possivel pra gente ajudar com a reuniao de Hackers no Brasil...estamos ai...!!
E novos artigos estao chegando...publicamos uma parte do BE...o glossario sobre a palavra hacker...Parece que o pessoal gostou..! :)

Mas depois a gente combina melhor...Parece que vai pintar o 1. encontro de usuarios do IRON BBS aqui na Baixada...pode ser uma oportunidade...valeu!
Por enquanto eh so...Inte+

| Waldemir Cambiucci |
| e-mail: waldemir@larc.usp.br |

| waldemir.cambiucci@iron.brasil.net |

From: Derneval R R da Cunha
Subject: Projeto "Hacker Crackdown" - Adendum

submeta hackers

Repetindo aviso: uns tempos atras tinha o projeto de traduzir o Hacker Crackdown. Fazer uma traducao meio mixuruca, mas legivel (pra nenhuma editora aproveitar em cima) e lancar nas BBSes e ftps da vida. Mandei carta pro Bruce Sterling e ele falou que acha a ideia otima, que posso fazer, nos moldes da versao que esta' disponivel em rede, ou seja, nao posso cobrar (nem tinha pensado nisso) pelo lance.

A ideia que desenvolvi e' mais ou menos essa: dividir a versao que ta' disponivel em n lugares na rede, em formato texto-Ascii, mas em arquivos de x paginas. E distribuir essas paginas para usuarios na rede que se interessarem em participar. A gente junta as paginas, bota o nome de todo mundo no topo e envia pela rede a quem pedir, coloca em BBSes, etc. O basico da ideia e' esse. Sei que ja' botei essa ideia antes na rede, mas por varias razoes nao fui adiante. Se o pessoal estiver afins, m e mande cartas e eu mando paginas p. pessoa traduzir. Nao precisa ser uma excelente traducao, nem mesmo boa, mas inteligivel. E ia facilitar p. pessoal da lista se inteirar do que e' ser fucador e talvez nao repetir os mesmos erros do pessoal la' nos s EUA.

Quem estiver afim de participar e' so' dar um toque. Se na sua area voce tem gente que pode participar, mas nao tem acesso a rede, avise e fique com um numero maior de paginas ou um capitulo inteiro, se for o caso. Quem me mandar mail sobre isso, coloque no subject: livro hacker, assim salvo a carta num folder separado. Quem quiser saber que raio de livro e' esse, procure no ftp.eff.org, subdiretorio pub/Publications/Bruce.Sterling/Hacker_Crackdown ou coisa do genero.

ADENDO

Ah, sim. A pessoa pode especificar o numero de paginas que pode traduzir, nao tenham vergonha de dizer que so' podem traduzir uma ou duas paginas por falta de tempo. Se se propor a dez paginas de cada vez, anda mais rapido. Sem um prazo especifico, mas tambem sem pagamento. E' algo p. ficar na historia e botar seu nome na lista de tradutores. Daqui a alguns dias mando as primeiras p. rede.
Inte'.

sig. Derneval R. R. da Cunha

OBSERVACAO: Sei que to repetindo a carta, mas ainda ha' vagas p. quem quiser participar.

From: "Guilherme K. Ramos"
Subject: Re: NormalMOO

submeta hackers

Singulares Leitores,

Estou participando a todos dessa lista que o NormalMOO (um Multi_Users Dimension Object Oriented) esta' com suas portas abertas. Um MOO e' uma especie de talker (viva a iniciativa do talker de Lord Morpheus!) com mais recursos. Os recursos que eu digo sao: aprender programacao

brincando. Outro dia li nesta lista que um garoto se dizia hacker pois na infancia desmontava brinquedos. Nos MOOs isso e' perfeitamente possivel desmontar os brinquedos que existem la' (claro que nenhum kid de $player vai poder alterar as permissoes de um brinquedo que nao e' dele). Desmontar eu entendo por tirar um raio-x do brinquedo sem estragar (comando @list :)

Na Internet World brazuca de dezembro sai uma materia sobre MOOs chamada `O MOO Veio para o Brejo'. Fiquem de olho.

De qualquer forma, todos estao convidados
(NormalMOO telnet://freire.futuro.usp.br 8888)

PS: Claro que telnet nao e' a forma ideal de entrar em um MOO. Isso se resolve com uma coisinha chamada client. Maiores informacoes, postar nesta lista.

`Greetings from Lake Tahoe' pra todo mundo

Subject: leiam

submeta hackers
   Como eh que leio a barata eletrica?

Subject: Re: leiam

submeta hackers

At 10:50 7/11/95 -0002, you wrote:
>   Como eh que leio a barata eletrica?

  Bom, para LER mesmo, vc pode usar um TYPE BE07.TXT | MORE do DOS, ou entao um MOST BE07.TXT;1 do VMS, ou um CAT do Unix. :)

  Agora, se vc se refere a abrir o pacote, bom, precisa do GZip.

  Caso vc tenha recebido o zine em UUENCODE ainda, tera' que desUUencodear antes de proceder a descompactacao com o GZip.

--Retirado do BE07--
Existe um descompactador no ftp.unicamp.br, oak.oakland.edu ou em qualquer mirror da Simtel, no subdiretorio:

/SimTel/msdos/compress/gzip124.zip
Uma vez descompactado o arquivo GZIP.EXE, a sintaxe seria:
                          "A>gzip -d arquivo.gz
--Retirado do BE07--

  Ok!?

  Qualquer problema, pode mandar mail direto pra mim ou pela lista mesmo.

CyA
 Renato
 drren@conex.com.br

Subject: (fwd) Re:Nova novela Globo

Excerpts from netnews.soc.culture.brazil: 8-Nov-95 RE:Nova novela Globo

by PAULO RICARDO@londrina.w
> MG>
> MG>Ola, ALL!
> MG>
> MG>A producao da Rede Globo esta boiando na Internet! Vejam so: no primeiro
> MG>capitulo, a heroina senta na frente do micro, da dois cliques e
ouve uma vo
> MG>"Cada ponto vermelho e uma pessoa ligada. Escolha com quem voce
quer falar.
> MG>
> MG>ai ela clica em um mapa, e faz cara de quem esta maravilhada. Se voces
> MG>observarem as imagens que aparecem no video, perceberao que a barra
de titu
> MG>traz "DARA.PPT".
> MG>
> MG>Gente, ela acessa a Internet com o PowerPoint!!! Eu quero esta versao do
> MG>software. Eh muito poderosa.
> MG>
> MG>PS. Eu so vi a novela de passagem. E foi justamente na hora em que
eu vi um
> MG>micro, que resolvi ver a cena. Ainda prefiro dar IBOPE para o Agente G.
> MG>

> Concordo com vocj, Mauricio. Pelo menos no Agente G AGENTE SABE o que AGENTE
> pode acreditar que i verdade ou i fantasia :-) . A Globo ta Brincando de
> Internet. Vai ver que a culpa i da EMBRATEL que nao liberou a linha ate o
> inicio da novela :-). Quem sabe eles emprestam o endereco do Fantastico para
> os atores brincarem de Internet, ja que o dia do Fantastico nao eh o
mesmo da
> novela.
>

Voces acham que isso e novidade? Nao se lembram do filme Jurassic Park? Quando o dono da outra companhia fala com o programador pra mandar ele roubar os embrioes de dinosauro? Eles falam pelo computador (ou pelo telefone mesmo, nao me lembro bem) e se veem na tela. So que embaixo da imagem nota-se um "scroll bar"
passando, o que significa que nao era uma conversa ao vivo e sim um "QuickTime movie", um filmezinho que passaram na tela enquanto conversavam.

    Isso prova novamente que o Mac ta sempre alguns anos `a frente do PC, ate em falsificacao da internet! :)

            ---Marcos.

    From: drren@conex.com.br (Renato Abel Abrahao)
    Subject: Barata 7

    submeta hackers

    Heya people,

    Ja' recebi o Barata Eletrica 07.

    Quem quiser, mande mail para mim, especificando o numero do
    zine e o formato que quer receber.

    Atualmente estou com suporte para MIME 1.0, BINHEX e UUENCODE

diretamente.

Nao estou enviando o zine diretamente em ASCII devido ao tamanho,
visto que meu acesso aqui e' COMMERCIAL e cada minuto pra mim
e' precio$o. :)

Te' mais pessoall,

._____
(Porto Alegre - Rio Grande do Sul - Brazil ___
(.
.) Conex Brasil Internet Provider)) - -=> Renato Abel
Abrahao)
(_____ _____ _____ / / - -=> drren@conex.com.br
(.
.) PGP Public Key avaliable (KeyID DA4233AD)
)
(FingerPrint: 75 9A C6 88 9F A8 9B 2E 45 8B 48 78 DF 33 19 E5
(.
.)_____
__)

COMENTARIO DO EDITOR: Valeu, Renato. Que mais posso falar?

From: Eliz
To: Derneval R R da Cunha
Subject: Veja se gosta:) Vers 2.0 (fwd)

Date: Tue, 14 Nov 1995 00:50:52 -0200
From: ??????? ?. ?????? -??????-
To: aessilva@carpa.ciagri.usp.br
Subject: Veja se gosta:) Vers 2.0

Hi Eliz:
Lembra do testiculo (small text) abaixo?
Pois e'. Sucesso. A tchurma gostou.
E' um texto sem bullshits nem papo furado de jornalista.
Foi escrito por quem e' do ramo. Great!
Achei ate um barato as drogas e vitaminas.
Usei umas quando tinha que rachar pras provas da Poli
e da Fisica (USP). Mas ja e' o passado.
E estou aqui porque estou interessado nos
"outros numeros ate o 6". Vc pode me envia'-los?
Sou prof da FGV (nao hacker) mas lido com computaria
(inclusive em Assembler e C) pra tese de dout.
Donde o interesse.
Tambem sou da USP como vc (true?)

Thanks a lot.

??????.

PS:
Se precisar de algo (que nao seja virus nem $$$) let me know.
Plim plim.

Derneval, to mandando pra tu ver um dos efeitos do Barata Eletrica:)

Pensa, nao acaba com o BE nao!:)
Nao esqueca de me avisar se for fazer encontro. Eu dou um jeito e apareco.
Um beijao:*

COMENTARIO DO EDITOR: E' sempre legal ver gente elogiando nosso trabalho e principalmente dar uma forca, quando o desanimo chega. De vez em quando me vem a cabeca dar uma parada no BE. To perdendo aula, talvez ate' provas por conta dele.
Prometo que vou *tentar* continuar ate' alem do numero dez.
Mas, para aqueles que quiserem curtir outros zines, ai' vao alguns enderecos, gracas ao Leandro do Alternetive (http://www.ufsm.br/alternetive/zine).
Nao conheco nenhum deles, nem seus autores. Mas apoio a livre expressao.

* Phobus
  R. Hebreus, 123 - Ipatinga - MG - 35164-170
* Coffin Cafe
  Cx. Postal 1217 - Joinville - SC - 89204-440
* R.D.N.
  R. Angelo Uglione, 1519/601 - Santa Maria - RS - 97010-570
* Falencia Fraudulenta
  Freire Alemao, 475/406 - Porto Alegre - RS - 90450-060
* Radicais Ideias
  Cx. Postal 9600 - Porto Alegre - RS - 90510-000

BARATA ELETRICA - Caixa Postal 4502 - CEP 01061-970
Sao Paulo - SP (e' possivel que ele vire edicao em papel, com esse ou outro nome)

PROXIMA REUNIAO DE HACKERS

Ou tentativa, que sera' provavelmente num boteco aqui perto da USP. Claro. Fica facil hospedar alguem, se necessario, da' p. pegar um onibus da rodoviaria facil (so' pegar o metro, direcao JABAQUARA, ate' a estacao SE', depois fazer a baldeacao p. direcao BARRAFUNDA, descer no metro REPUBLICA, la' fica o ponto de onibus CIDADE UNIVERSITARIA. A partir dai, e' so' descer depois da ponte. E' naquela area - nao esqueca de anotar o endereco que sera' distribuido na rede). Talvez seja na esquina da R.Agostinho com Desembargador Fairbanks, mas nao esta' garantido. Mandem um mail.

Ia ser num lugar chamado CAFE' COM LEITERNET, que fica na Fradique Coutinho, quase esquina com a rua Wizard. Mas o lugar, apesar de ser um Cybercafe', nao tem muito espaco p. sentar. O micro, que as sextas-feiras fica conectado a rede, via telefone, tem uma plateia enorme. Digo plateia porque na primeira vez que fui, tinha um cara, que vou chamar de "Doponto", latia um "perai, so' mais um tempo" e nao largava do teclado. Nem o Artur tinha coragem de puxar o cara de la'. Como tinha que ir embora, usei um pouco de psicologia "canina". Cheguei no dito e falei, usando um linguajar "delicado", sem ameaca. Estragou a noite, mas valeu. Consegui mostrar minha entrevista, feita pelo Leandro da Alternetive (http://www.ufsm.br/alternet/zine/be.html) pro dono do estabelecimento. Que adorou o visual html do Alternetive, mas nao se convenceu ate' hoje a ler o Barata Eletrica. Na outra vez que fui, o tal "doponto" (ex-colega de amb.de trab) nao tava na maquina, mas tava afins de gozar com a minha cara. Capoeirista e' assim. Quer te deixar nervoso pra fazer voce cair nele. Ai', se ele conseguir se virar, e' defesa pessoal. Caso contrario, e' artigo 129, acho. Agressao por motivos futeis. Sem falar que isso ia realmente estragar a noite. Prefiro ir para outros bares la' perto (tem 1 monte), do que ficar nesse clima.

Mas voltando ao lugar, tem sua atmosfera..nao e' ruim.

Parece que o FINNEGAN'S aqui em Sampa tambem tem esse lance de

Cybercafe', com micros e tudo. Mas nao fui la' pra checar e me parece ser um lugar meio caro.

BIBLIOGRAFIA:

O texto sobre "Batalha pela Mente" veio inteiramente da minha cabeca, fruto da leitura de alguns livros, tais como "1984", "Admiravel Mundo Novo" e "Volta ao Admiravel Mundo Novo" do Aldous Huxley e "Hidden Persuaders" que foi traduzido como "Tudo o q. voce queria saber sobre propaganda"
Gracas a uma colabaracao via net do Joao Cesar, posso acrescentar esses outros livros.
Propaganda Subliminar Multimidia - Flavio Calazans Editora Summus.
A era da Manipulacao - Wilson Bryan KEY Editora Scritta
A Natural History of The Sense - Diane Ackerman Vintage Books
Uma leitura recomendavel tambem e' a "Morte do Professor Antena", do autor portugues

A materia sobre o CCC foi algo mais dificil. Tive que ir la' e ainda assim ficou faltando muita coisa pra falar. Eles tem uns dez ou doze anos de historia, po^! A(s) pagina(s) deles na Web tem uns links otimos.
URLs:

http://www.artcom.de/ccc
http://www.zerberus.de

Sobre o "Zagreb Diary". Ver abaixo:

Zagreb Diary can be found on a lot of different electronic networks, it is copyright free and can be ported to any network or other means of communication you like, but please drop my a line, you can reach by sending a message to wam@zamir-zg.comlink.de or wam@zamir-zg.comlink.apc.org. Zagreb Diary is dedicated to Tyche, Pjort and Rik, so that they found out what there father have been doing all that time in Zagreb.
Financial support for Grassroot relief work in Croatia or BiH can be send to Kollektief Rampenplan (atn. Lylette, Postbox 780, 6130 AN Sittard, Netherlands, tel:. +31-46-524803 and fax: +31-46-516460 or to Zagrebacka Banka, Zagreb, accountnr.: 2440291594, to Kat, Pieter Jan Herman Fredrik, Brace Domany 6 6fl nr3, 41000 Zagreb.
Please notify me if you send or have send any donations.

A materia do John Markoff, que apesar de bem escrita e tal, vou logo avisando de que o mesmo nao e' exatamente elogiado no computer underground por conta da grana que ele faturou em cima do Mitnick. Pra conseguir outra reportagens da Wired, mande mail p. info-rama@wired.com ou info@wired.com com help no corpo da mensagem. E' possivel depois pedir que mandem arquivos pelo correio eletronico. A revista wired tem uns artigos bons sobre hacking, mas nao e' uma revista p. hackers, bom especificar. URL: http://www.wired.com

A reportagem da Bulgarian Virus Factory costumava ter em todo "mirror" da Simtel no subdir pub/virus. Hoje, so' se encontra no arquivo: bulgarian.factory.doc
ftp://info.cert.org/pub/virus-l/docs
E' considerada antologica, mas nao atual. Fala-se muito de "Mutation Engines". O Bontchev me deu permissao p. republicar, nao pude traduzir por falta de tempo, o que e' pena. Tem uma pa' de outros artigos bons no URL

acima, sobre o tema.

Sobre as cartas, a maioria veio da lista hackers, outras da informatica-jb, etc A "oracao" me foi enviada de uma lista de piadas.

Sobre o filme THE NET maior parte e' escrito de cabeca, com partes tiradas de outras publicacoes. Mas p. quem quer, ai' vai uma bibliografia interessante, tirada do Netsurf Digest.
http://www.netsurf.com/nsf/v01/03/nsf.01.03.html

An introduction to some cipher systems
http://rschp2.anu.edu.au:8080/cipher.html

Lawrie's Cryptography Bibliography
http://mnementh.cs.adfza.oz.au/htbin/bib_lpb

Materials from "Applied Cryptography" by B. Schneier
http://www.openmarket.com/info/cryptography/applied_cryptography.html

Cryptography FAQ from sci.crypt
http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html

The Cyphernomicon - A Cypherpunk's Guide to Cryptography and Privacy
ftp://ftp.netcom.com/pub/tc/tcmay/CP-FAQ

DES
http://www.rsa.com/rsalabs/faq/faq_des.html

The Challenge to Decrypt a Secure Netscape Transaction:
http://www.netsurf.com/nsf/v01/03/local/nscpchal.html

RSA FAQ
http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/part06/faq.html

RSA in 17 lines of Perl
http://draco.centerline.com:8080/~franl/crypto/rsa-guts.html

The RSA-129 Challenge
ftp://ftp.ox.ac.uk/pub/math/rsa129/rsa129.ps.gz

Public Key Cryptography FAQ
http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/part06/faq.html

Key Management
http://www.rsa.com/rsalabs/faq/faq_km.html

PGP Public Key Server
http://www-swiss.ai.mit.edu/~bal/pks-toplev.html

Key Certificate Issuance System
http://www.rsa.com/rsa/prodspec/cis/rsa_cis.htm

Internet Regional Policy Authority (IRPA)
http://bs.mit.edu:8001/ipra.html

RSA FAQ on MD2, MD4, and MD5, and Digital Signatures
http://www.rsa.com/rsalabs/faq/faq_misc.html

Steganography Archives
ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/

Digital Notary Systems
http://www.surety.com

Visa Announces Smart Card Specification
http://www.visa.com/visa/press_releases/visa_pr5.31.95.a.html

Mastercard and Visa Announces Secure Credit Card Transactions
http://www.mastercard.com/Press/release-950623.htm

Chaum's Article on Blind Signature Technology and Digital Privacy
http://www.digicash.com/publish/sciam.html

Proposed Electronic Payment Systems
http://ganges.cs.tcd.ie/mepeirce/Project/proposed.html

Mondex Stored Value Card
http://www.mondex.com/mondex/home.htm

Remailer FAQ
http://www.well.com/user/abacard/zremail.html

Remailers Resource Page
http://www.cs.berkeley.edu/~raph/remailer-list.html

Breaking the Anonymity of anon.penet.fi
http://www.clas.ufl.edu/~avi/NII/TIME_penet.txt
http://www.tezcat.com/~wednsday/penet.pr

How to Secure Remailers Against Attacks
http://obscura.com/~loki/remailer-essay.html

CRYPTOGRAPHY

* "PGP: Pretty Good Privacy". Simson Garfinkel, O'Reilly and Associates, 1995.
* "Kahn on Codes: Secrets of the New Cryptology", David Kahn, MacMillan, 1983.
* "Seizing the Enigma", David Kahn, Houghton-Mifflin, 1991.
* "Applied Cryptography: Protocols, Algorithms, and Source Code in C". Bruce Schneier, John Wiley & Sons, 1994.
  Errata Sheet:
  http://www.webcom.com/~hurleyj/service/errata-appl-crypt.html
* "E-mail Security: How to Keep Your Electronic Messages Private". Bruce Schneier, John Wiley and Sons, 1995.
* "A Man Called Intrepid". William Stevenson, Harcourt Brace Jovanovich, 1976.
* "The Official PGP Guide". Philip R. Zimmermann, MIT Press, 1995.

PRIVACY

* "The Computer Privacy Handbook". Andre Bacard, Peachpit Press, 1995.
* "Who Owns Information? From Privacy to Public Access". Anne W. Branscomb, Basic Books, 1994.
* "Managing Privacy: Information Technology and Corporate America".

H. Jeff Smith. University of North Carolina Press, 1995.

EM PORTUGUES:

"O caso Mattia Pascal" - Luigi Pirandello
"Historia de Gorducho Entalhador" - Antonio Manneti
"O Alienista" - Machado de Assis
"Codigos Secretos" - Ed Melhoramentos