BARATA ELETRICA, numero 1
Sao Paulo, 23 de janeiro de 1994

Conteudo:

Creditos:

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

wu100@fim.uni-erlangen.de

Introducao:

Este e' o que chamo de primeiro numero (nao beta-teste).
Como isso aconteceu foi explicada no numero anterior, algumas
coisas como a origem do jornal, minha experiencia como Hacker e
a descricao da aparencia que o sujeito acaba tendo depois de 1
tempo grande na frente da tela de um micro. Varios me perguntaram
coisas relacionadas ao que e' Hacker, afinal de contas?

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

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

Nao da para definir o que e' realmente um hacker. Mas em qualquer sala de computacao existem aqueles que vao para trabalhar, aqueles que vao para aprender e aqueles que vao para se divertir. O Hacker faz tudo isso e ainda mais alguma coisa, um algo mais que nao da para definir. Existem os que chegam para um cara que sabe alguma coisa e suplicam: "me ensina a fussar?"

O verdadeiro fussador (ou fucador - estou escrevendo em sem usar acentos ou cedilhas para facilitar transmissao via Unix) ele nao precisa de aulas ou professor. No maximo um guru que ilumine a direcao. O caminho ele mesmo vai trilhar, dentro da especialidade que ele escolher.

Normalmente ele se define por alguma. Comeca aprendendo o que precisa aprender como os comandos do sistema

operacional que usa, seja ele Unix, Dos ou OS2. Claro que inicialmente ele nao vai muito longe. E' algo chato, mas necessario. Nem sempre esse aprendizado acontece de forma sistematica. Em um caso o sujeito aprende um comando ou outro entre sessoes de 8 horas mexendo com compiladores Pascal ou joguinhos, em outro caso a pessoa precisa saber como recuperar um arquivo perdido. Em outro caso, a pessoa nao aprende absolutamente nada, vai pegando jogos e programas com amigos ou em BBSes, ate que a necessidade realmente surge.

O contato constante com o computador e a vontade de fazer com que ele obedeca faz surgir o individuo "fussador", que despreza a ideia de frequentar um curso ou pagar a um profissional para que o ensine a usar um programa. Alguns fazem dessa facilidade com a maquina uma profissao e mudam de ramo. A vontade de explorar este universo eletronico transforma o individuo. O poder e um afrodisiaco.

Qualquer pessoa que tenha pelo menos lutado para aprender uma linguagem de computacao (PASCAL, C, CLIPPER, etc) pode entender o que e o prazer de ver um programa funcionando direitinho. A denominacao nao importa. O que importa e' conseguir fazer a coisa funcionar com o minimo de ajuda possivel ou faze-la funcionar alem do que os outros esperariam conseguir, como quando se consegue fazer o programa fazer algo que nao normalmente faria. Ou melhor dizendo, dominar o programa.

Um pouco de historia:

Os primeiros computadores que chegaram aqui no Brasil, baseados no processador ZX-80 continham poucos programas. Basicamente o unico uso que tinham era o de aprender a linguagem BASIC ou o ASSEMBLY. Haviam os jogos e programas que se podia comprar, mas nao muitas lojas. Usar um computador para movimentar um negocio, como banco de dados ou editor de textos as vezes significava conseguir um programa em BASIC para fazer o banco de dados ou o editor de textos. Quando eu tinha 19 anos, parado na porta de uma loja ouvi a vendedora comentando de um garoto de 15 anos que tinha o seu escritorio de venda de programas. "Comecou aos 11, com um micro de 2 Kbytes de memoria". E' , naquele tempo a impressora do micro era mais cara do que o proprio e o drive de disco 5 1/4 nao era mais barato. No entanto, eu me recordo ter lido numa VEJA que os empresarios na epoca queria levantar uma brecha na legislacao de reserva de mercado (que proibia qualquer tipo de importacao de industrializado eletronico, a lei de reserva de mercado para informatica estava em projeto) para poder importar esses micros em quantidade.

O cara aprendia na marra. E era obrigado a fazer seus proprios programas, encontrar quem podia ajudar com esta e aquela dica era outro problema. Depois descobria que os programas em BASIC eram muito lentos e resolvia apelar para a ignorancia(?) aprendendo linguagem de maquina, ate' que chegava a conclusao de que pagar um menino de 15 anos para fazer a coisa nao era uma ideia ma'. As lojas deixavam criancas "praticarem" com o material de venda, provavelmente para fazerem os adultos pensarem que era

coisa facil ou estimular as vendas para criancas.

Tinha uma enciclopedia chamada INPUT, que era a maior atracao, com aulas de programacao em BASIC e dicas para fazer programas e joguinhos. Era muito completa e dificil de encontrar nas bancas. Tinha o trabalho de trazer programas que respeitavam as diferencas de compatibilidade entre os varios computadores disponiveis no mercado e os truques para se fazer bancos de dados em fitas K-7, ja' que era muito dificil de se encontrar alguem que usasse disk-drive.

Para um jovem era facil conseguir uma certa habilidade em programacao (comparado com um profissional qualquer) e em conseguir informacao, ja' que os pontos de reuniao eram a loja de computacao ou o fliperama. Um primo meu aprendeu BASIC em casa, com um livro qualquer e ia treinando em lojas de informatica, onde tambem encontrava outros na mesma situacao. Copiar joguinhos significava aprender a destravar a protecao que o jogo tinha contra copia indevida. Criar um jogo estimulava o desenvolvimento de um programa de protecao. Quem aprendia linguagem Assembly de um ZX-80 aprendia em pouco tempo a linguagem Assembly do PC-XT ou AT, muito menos complicada. Computacao vicia.

Os micros dos sonhos naquele tempo eram o CP500, com disk-drive e o Apple. Pena que o Apple, fosse qual fosse esquentava apos uso intensivo, congelando qualquer aplicativo e impedindo o salvamento do arquivo.. Ate' hoje ele guarda porem uma legiao de fas, como mostra um programa, que emula o funcionamento de Apple num XT e um grupo de discussao so' sobre Apple][e. Durante muito tempo foi aquele micro dos sonhos, que custava 2000 dolares na sua configuracao ideal, com dois disk-drives e uma impressora Amelia ou outra qualquer. Num tempo em que a maioria dos usuarios de micros usava um velho televisor como monitor, esse micro tinha um monitor de fosforo verde, coisa chique, porque era mais rapido de ligar.

Que tempo foi esse? Em 1988 ainda era algo caro de se comprar nas lojas de informatica. Ha' 3 meses um amigo me perguntou qual o preco atual para um micro desses em bom estado e se servia para aprender informatica. Obvio que nao gostou da resposta. Parece que o cunhado tinha vendido o carro para poder comprar o micro e a impressora. Coisas da vida, fazer o que?

(continua)

NOTICIAS DA RATAIADA

O sucesso da lista de Hackers

A lista de Hackers da esquina-das-listas e' um sucesso, atingindo ja' um numero em torno de 20 fuc,adores e aumentando. Para quem nao sabe:

Todos os comandos relativos a lista sao simples e envolvem escrever para esquina-das-listas@dcc.unicamp.br (a linha de subject nao tem importancia). Em seguida:

Para se inscrever e' preciso escrever na carta:

inscreva hackers seuemail@xxx.xxx.xxx

Para submeter qualquer coisa a correspondencia tem que ter no topo:

submeta hackers

Quem quiser ver seu nome listado escreve:

usuarios hackers

OBSERVACAO: Deve haver obrigatoriamente uma carta-resposta automatica acusando recebimento da mensagem.

IRC ainda nao, mas TALKER sim

Uma novidade da tchurma e' a abertura de um talker especifico para a rataiada. Para quem nao sabe, o negocio e' fazer o telnet para acessar, da seguinte forma:

telnet carpa.ciagri.usp.br 3000

O 3000 e' necessario para se chegar ao talker. Depois existe o pedido de um usercode, que o novato pode inventar e o password, para ter exclusividade do codinome adotado.

Comandos uteis:

Uma vez dentro, existe uma listagem do pessoal que esta' na antecamara e o individuo pode comecar a entrar no papo. Qualquer coisa que digitar sera' transmitida aos outros participantes apos a tecla Enter ser pressionada. A frase aparecera' na tela com o nome da pessoa que digitou na frente.

.help new - da' ao usuario iniciante uma relacao dos comandos mais usados.
.shout "To aqui" - a frase "To aqui" ecoara em todos os lugare do ambiente Se voce combinou com alguem, esse alguem podera' te encontrar e te chamar depois.
.quit - para sair

Notar que os comandos sempre sao precedidos de . do contrario, passa a ser interpretado como frase.

O local dispoe de ambientes privados onde so' se podera' entrar com convite. Lembra um MUD, mas nao e' um local onde se joga, so' para bater papo.

A ideia e' reunir principalmente gente que tenha como ponto em comum esse vicio por informatica ou elementos relacionados a cultura "Hacker", como seguranca de computadores, privacidade, problemas com virus de computador, dicas e truques para isso e aquilo, etc..

A ideia foi de MWalder, que seguiu o exemplo que fiz criando a lista hackers na esquina-das-listas. Agora, o negocio e' torcer para bastante gente se conectar ao Talker e lancar as bases do que espero mais tarde ser o proximo encontro de Hackers em Sao Paulo.

Para quem nao leu a versao Beta-teste do jornal, a ideia e' fazer a rataiada, todos os fucadores de micro se reunirem, senao em

Sao Paulo, nas suas cidades mesmo, criando grupos, trocando ideias, ate' que haja grupos espalhados por todo o pais. Ai' sera' a hora de termos a primeira reuniao internacional de Hackers do Brasil.

COMO CRIAR UM GRUPO DE RATOS DE COMPUTADOR?

Nessas ferias, aconteceu um encontro de estudantes de Comunicacao. Numa de penetra, entrei numa festa e apesar da quantidade de mulher, encontrei um pessoal que me apresentou ao Ailton da UFMG. Conversa vai, conversa vem, entramos naquele papo incrivelmente chato que e' as possibilidades da Internet no Brasil e a futura reuniao de Hackers brasileiros e internacionais. No meio de tanta mulher, conversar sobre isso..

Nos dias seguintes, foi o lance de trocar informacoes. Ele sabia, conhecia varias pessoas que tem essa fixacao por computador. Tinha a ideia de montar o grupo, mas nao o como fazer a coisa. Eu tinha Megabytes e Megabytes de material altamente significativo sobre o assunto, armazenado em dois anos de pesquisa na rede Internet, mas so' a ideia de montar uma lista e' que tinha vingado. Pensando e pensando no assunto, cheguei a algumas conclusoes:

* O mais importante e' a vontade de sair e trocar experiencias com outros "micromaniacos". O rato de laboratorio sozinho vai gastar uma enorme quantidade de tempo (sem trauma ou reclamacao) para aprender coisas que depois poderiam enriquecer a experiencia de varios outros. Sem transmitir, essa experiencia morre com ele.

* Nos Estados Unidos e na Argentina (como em outros lugares do mundo) ha' lugares, listados na revista 2600 (ver abaixo) onde se pode encontrar todo primeiro sabado do mes, gente que se reune para trocar ideias sobre computadores. E' necessario criar um ponto de reuniao e divulgar sua existencia, para que gente de fora possa entrar e participar (mesmo que seja p. ouvir apenas).

* Ha' a necessidade de jornais em formato eletronico ou zines do assunto. E' preciso que haja um veiculo de comunicacao motivador de pesquisas ou moderador de disputas, um orgao para registrar o que foi falado ou o que esta' rolando. Muita gente pena para aprender montes de programas, mas apenas anota num pedaco de papel um ou outro comando "que nao pode esque--cer" e depois joga fora. Um ano depois nem se lembra mais. E era uma dica que valia a pena.

* No caso de formacao de um grupo, pode ou nao haver a especializacao: Cada pessoa do grupinho escolhe uma area de atuacao onde ninguem se mete: linguagem C, Winword, Sistema Operacional, Internet, etc
Ou pode o grupo inteiro se especializar naquilo. Colocar uns rumos e' interessante, para se evitar a duplicacao de material.

* O ideal e' que todo mundo fizesse um esforco para traduzir um ou outro lance interessante, tanto do ingles pro portugues como vice-versa. A Internet esta' chegando no Brasil e o material daqui, no futuro, pode ser veiculado mundialmente. Quando fui na Argentina, os argentinos que me receberam preferiram de cara falar em Ingles comigo. Evitava o trabalho dos dois lados, de entender o que se estava falando. Mas eu comecei a ler em ingles ha' muito tempo para chegar a esse ponto. Por outro lado, quem traduzir pro portugues algum documento, pode acrescentar seu nome a ele e auferir alguma fama com isso. Nao que

eu recomende pensar que isso vale alguma coisa, mas se for algo util, e for distribuido em BBSes pode quem sabe valorizar o Curriculo Vitae.

* Ninguem tem que perder seu tempo bancando o professor, mas pode-se intercambiar experiencias. Uma coisa que costuma acontecer e' eu saber usar Unix, mas nao saber coisa alguma de portar um programa em "C" para computadores de grande porte. Esse intercambio ajuda muito.

O texto abaixo eu produzi com a ajuda de varios amigos, muitos deles sumidos. Provavelmente, nao se recordam de tudo o que me falaram. Como eu anotei, muita coisa do que esta' abaixo e' experiencia viva, e nao extraida de algum livro, embora hajam muitas referencias a textos que consegui na rede Internet. A base que me deu um "faro" para o assunto veio desse tipo de conversa, meio exclusiva de gente capaz de perder alguns anos da vida na frente da tela de um computador. Foi esse tipo de contato humano que possibilitou-me continuar aprendendo e ingressar na Internetcidadania que e' o meu trabalho atual, sem perder o gosto, coisa comum de quem se profissionaliza.

VIRUS DE COMPUTADOR

(* Observacao: Nao me considero responsavel pela ma' aplicacao de qualquer dica colocada aqui. Mexer com virus de computador e' algo traicoeiro, na melhor das hipotese. Ja' tive a desagradavel experiencia de ir "limpar" os virus de um computador de uma pessoa proxima e sair da casa dela com a suspeita (no ar) de que esse virus tinha vindo dos meus disquetes. Eu sei que sou inocente. mas provar isso e' muito dificil. Pode acontecer. *)

Existe pouca literatura sobre isso no Brasil. Alguns muito tecnicos outros apenas descritivos, outros com medo de ensinar algo que estimule as pessoas a terem ideias. Um ou outro ensinam como fazer isto e aquilo e como remover usando um removedor de virus de sua autoria. Como os virus de computador sao objeto de aperfeicoamentos, muita informacao que ja' foi escrita sobre o assunto ja' ficou quase que completamente obsoleta.

Antigamente (ate' a versao 88, creio), o antivirus SCAN trazia um arquivo contendo todas as novas modificacoes em relacao a ultima versao e geralmente ate' descricoes dos virus des-infectaveis. Mas e' raro alguem que se preocupasse em ler ou guardar a versao completa do Scan com todos os arquivos. Falo desse programa porque foi durante muito tempo o unico antivirus disponivel.

As primeiras referencias a palavra virus de computador no Brasil na imprensa apareceram por volta de 88-89. Ninguem entendia muito disso. Havia o caso do WORM, que foi noticiado na Manchete, mas so' em 89 comecou a infestacao dos micros de forma geral e o aparecimento de referencias na imprensa. Nao havia inclusive solucao. Falava-se em nao copiar programas de origem desconhecida (ao que um amigo que assumia sua preferencia pela copia de programas falou: eu so' pirateio de quem eu conheco, entao ta tudo bem). No uso de software de protecao e o famoso uso da etiqueta que impede a gravacao. Tudo bem que o unico software antivirus era o Flu-Shot+ e uns programinhas home-made ou USP-made

ou feitos sei la' onde. Algumas vezes, por mal uso, o proprio programa continha o virus que prometia limpar. As pessoas eram obrigadas a ter varios tipos de programas antivirus para cada um dos que existiam.

Provavelmente o que mais popularizou o Scan e o Clean como antivirus foi essa preocupacao com a atualizacao e gratuidade para o usuario. De tempos em tempos era um item de troca, ter a versao mais atualizada, entre Piratas e copiadores de software. Ao contrario de softwares como o Word, Wordstar e outros, ate hoje seu uso permanece pratica--mente o mesmo.

Bom, comecando com o trabalho:

Definicao:

Antes de mais nada, e' preciso dizer que praticamente qualquer coisa de errado que acontece com um computador durante uma sessao de trabalho e' atribuida a um virus, independente da causa estar no programa ou na falta de experiencia do usuario. De acordo com uma pesquisa da PC Magazine, 50 % dos prejuizos em software sao culpa de mal uso ou inexperiencia. Qualquer um que atualize o software sabe os problemas de reaprender a mexer com novos botoes de salvamento de trabalho ou teclas de saida e apagamento que colidem com o uso antigo de outro software. O usuario inexperiente destroi muito mais dados do que qualquer virus.

Mesmo programas bem desenvolvidos tem defeitos que destroem o trabalho por conta de alguma falha no lancamento. Normalmente sao as versoes X.0. Qualquer pessoa que utilize um software recem-lancado (normalmente numero ponto zero) se arrisca a ter dores de cabeca que nao serao culpa de virus de computador e que ninguem sabera' como resolver. A versao 5.01 de qualquer programa e'quase sempre a versao com correcao dos erros encontrados na versao 5.0. Para quem nao acredita e' so' perguntar a alguem que comprou a versao 6.0 do Wordperfect para Windows logo quando saiu. Ou a versao 6.0 do MSDos, a versao 3.0 do Windows, ou a versao 5.0 do Clipper. Saiu um artigo na folha de Informatica do Estado de Sao Paulo (13/02/94) falando sobre o Pentium e tambem como alguns softwares recem-saidos podem apresentar defeitos, ou bugs, tao destrutivos quanto um virus.

Um virus de computador e' um programa que pode infectar outro programa de computador atraves da modificacao dele de forma a incluir uma copia de si mesmo (de acordo com Fred Cohen, autor de "A Short Course on Computer Viruses"). A denominacao de programa-virus vem de uma analogia com o virus biologico, que transforma a celula numa fabrica de copias dele.

Para o publico em geral qualquer programa que apague dados, ou atrapalhe o trabalho pode levar a denominacao de virus. Do ponto de vista de um programador, o virus de computador e' algo bastante interessante. Pode ser descrito como uma programa altamente sofisticado, capaz de tomar decisoes automaticamente, funcionar em diferentes tipos de computador, e apresentar um indice minimo de problemas ou mal-funcionamento. Stephen Hawking se referiu ao virus de computador como a primeira forma de vida construida pelo homem. De fato: o virus e' capaz de se reproduzir sem a

interferencia do homem e tambem de garantir sozinho sua sobrevivencia. Como a auto-reproducao e a manutencao da vida sao para alguns cientistas, o basico para um organismo ser descrito como vivo. O virus Stoned e' um exemplo que resiste ate' hoje, anos depois da sua criacao.

Sendo o virus um programa de computador sofisticado, ainda que use tecnicas de inteligencia artificial, ele obedece a um conjunto de instrucoes contidas no seu codigo. Portanto e' possivel se prevenir contra seu funcionamento, conhecendo seus habitos.

Bomba Logica e Cavalo de Troia

O cavalo-de-troia se assemelha mais a um artefato militar como uma armadilha explosiva ou "booby-trap". O principio e' o mesmo daquele cigarro-explosivo ou de um daqueles livros que dao choque. Nao se reproduz. A expressao cavalo-de-troia tambem e' usada para com programas que capturam senhas sem o conhecimento do usuario. O criador do programa pode usufruir da senha de acesso capturada.
Um exemplo de bomba-logica e' um arquivo texto "armadilhado" que redefina o teclado ao ser lido pelo comando TYPE. Em um exemplo classico, o sujetio digita:

```
C:\> type carta.txt
```

Os codigos acrescentados ao texto alteram a tecla x (ou qualquer tecla, nao importa) de forma que, ao inves de escrever x na tela ela aciona uma macro que ativa a formatacao do disco rigido.

Existe um software, chamado CHK4BOMB, disponivel no subdiretorio msdos/virus de qualquer "mirror" do Simtel20 que ajuda a detectar a existencia desse tipo de programa. Os antivirus comuns dificilmente detectam, a nao ser em casos mais famosos.

Modus Operandi

Ate' algum tempo atras, os virus se dividiam em dois grupos principais:

Virus de disco - ex: Stoned, Michelangelo, Ping-Pong

Infectam o BOOT-SECTOR. Esta e' a parte do disco responsavel pela manutencao dos arquivos. Da mesma forma que uma biblioteca precisa de um fichario para saber onde se encontram os livros, um disco precisa de ter uma tabela com o endereco dos dados armazenados. Qualquer operacao de entrada e saida (carregamento ou salvamento de um arquivo, por exemplo), precisaria do uso dessa tabela. Salvar ou carregar um arquivo num disquete infectado possibilitaria a ativacao do virus, que poderia infectar outros disquetes e o disco rigido.

Virus de Arquivo - ex: Jerusalem, Athenas, Freddy

Infectam arquivos executaveis ou de extensao .SYS,
.OVL, . MNU, etc. Estes virus se copiam para o inicio ou fim
do arquivo. Dessa forma, ao se chamar o programa X, o virus
se ativaria, executaria ou nao outras tarefas e depois
ativaria o verdadeiro programa.

Atualmente existem uma terceria e quarta categorias

Virus Multi-partite- ex: Whale, Natas

Infectam tanto o disquete quanto os arquivos executaveis.
Sao extremamente sofisticados.

Virus como o DIR-II

Alteram a tabela de arquivos de forma a serem chamados
antes do arquivo programa. Nem propriamente dito sao
FILE-INFECTORS nem sao realmente BOOT-INFECTORS muito menos
multi-partites.

Outras caracteristicas e um pouco de historia:

Virus residentes e nao-residentes:

Os primeiros virus eram de concepcao muito simples e
funcionavam como programas auto-reprodutores apenas. O
usuario usava o programa infectado, acionava o virus, que
infectava todos os outros programas no subdiretorio (virus
cacadores, que procuram programas em outros subdiretorios
sao muito bandeirosos) e depois colocava para funcionar o
programa (o que o usuario realmente queria usar). Ponto
final. Se um programa nao infectado for acionado, ele nao
sera' infectado.
Os virus residentes, mais sofisticados permanecem na
memoria apos o uso do programa infectado. Portanto podem
infectar qualquer outro programa que for chamado durante a
mesma sessao de programacao, ate' que o computador seja
desligado. Como o sistema operacional e' basicamente um
programa destinado a tornar comandos como DIR, TYPE, etc
inteligiveis para os chips do computador, ele se torna
objeto de infeccao. Neste caso, toda vez que o computador
for ligado, o virus sera' carregado para a memoria, podendo
infectar qualquer programa que for usado.
A grande maioria dos virus atuais pertence a este tipo de
virus.

Quanto a deteccao:

Stealth - ex: Athenas, 4096, GenB, etc

Um virus, como todo programa ocupa espaco em disco. O
codigo, em linguagem de maquina, mesmo ocupando um espaco
minimo, aumenta o tamanho do arquivo. Ao se copiar para

dentro do programa a ser infectado, duas coisas aconteciam: o programa aumentava de tamanho e alterava a data de gravacao. No caso do virus Jerusalem, por exemplo, o programa "engordava" a cada execucao, chegando a se auto-infectar ate' tamanhos absurdos.
Para checar se o arquivo estava infectado era so' fazer uma copia do mesmo e acionar esta copia. Depois bastava executar o comando "DIR" e o resultado mostraria que a data, hora de criacao e o tamanho do programa eram diferentes.

Com o 4096, isso nao acontecia. Uma vez residente na memoria, o virus checava para a existencia de uma copia sua no arquivo .exe ou .com e restaurava uma data quase identica de criacao de arquivo. Dessa forma, so' um antivirus ou um usuario atento descobria a diferenca.

O virus ATHENAS ja' e' algo mais sofisticado. Ele altera tudo de forma a evitar que um Antivirus detectasse a diferenca. Em outras palavras, seria necessario que o virus nao fosse ativado para que fosse detectado. Se o arquivo COMMAND.COM fosse infectado, todos os arquivos .com ou .exe de um disco rigido seriam infectados, cedo ou tarde. O usuario poderia usar o antivirus que quisesse. O virus continuaria invisivel. Dai o uso do adjetivo "STEALTH", do aviao americano invisivel ao radar.

Como alguns desses virus verificam ate' se ja' estao presentes na memoria, o funcionamento do computador nao diminuiria de velocidade o suficiente para alertar o usuario.

OBSERVACAO: Uma vez que o virus Stealth esconde sua presenca de qualquer programa antivirus, uma forma de descobri-lo e' justamente guardar um disquete com o programa infectado. Se o programa antivirus do micro "suspeito" de infeccao nao o descobrir a presenca de virus no disquete, entao provavelmente o micro esta' infectado. Isso funciona principalmente com versoes mais novas de um mesmo virus, como o Athenas, o GenB (vulgo Brasil), etc..

Companheiros (Companion)

Sao virus que nao infectam programas .exe. Ao inves disso criam um arquivo de extensao .com, cujo o atributo e' alterado para Hidden (escondido). Como o arquivo .Com e' executado antes do .exe, o virus entra na memoria e depois chama o programa. E' facil e dificil de detectar. Por nao alterar o programa, escapa a algumas formas de deteccao, como a checagem do CRC. Teoricamente um comando DIR teria poder para descobri-lo: DIR /AH mostra todos os arquivos escondidos. Mas para se ter certeza, so' quando o BOOT e' feito com um disquete limpo de virus, ja' que nada impede de um virus Companion ser tambem Stealth (ou poli-morfico, ou multi-partite, tem virus para todos os gostos).

Polimorficos - ex: Natas, Freddy, etc

No tempo em que os primeiros antivirus contra o Jerusalem apareceram, alguns "espertos" resolveram criar novas versoes indetectaveis atraves da alteracao do virus.

Como o antivirus procura uma caracteristica do virus para dar o alarme, essa modificacao obrigava a criacao de um novo detector de virus. Isso e' bastante comum. Novas versoes de virus sao feitas a cada dia, aproveitando-se esqueletos de antigas versoes, tendo alguns virus gerado verdadeiras "familias" de "parentes", de versoes mais antigas. O proprio virus Michelangelo seria uma versao "acochambrada" do virus Stoned.

A ultima moda (para os projetistas de virus) e' o uso da poliformia. O virus se altera a cada vez que infecta um novo arquivo. Dessa forma o virus cria N variacoes de si proprio. Hipoteticamente, se uma variacoes escapasse ao antivirus, ela poderia re-infectar todos os arquivos novamente.

Retrovirus - ex: Goldbug, Crepate

Sao virus que tem como alvo antivirus, como o Scan, Clean, CPAV NAV, ou qualquer arquivo que contenha as strings AV, AN, SC, etc no nome. Pode ser o objetivo principal ou paralelo. O Crepate, por exemplo, e' multipartite (infecta tanto o boot como arquivos executaveis). Alguns simplesmente deletam os arquivos que contem o CRC dos programas analisados (uma especie de selo que alguns antivirus, como o NAV, por exemplo, criam: um arquivo onde varias caracteristicas pre-infeccao (tais como tamanho, data, atributos) ficam armazenadas). Um ou outro anti-virus tem codigo p. desativar anti-virus residentes, como o V-SHIELD e o VACINA e passar desaper -cebido.

Virus-anti-virus

Existem virus que se especializam em detectar e infectar arquivos ja' infectados por outros virus menos sofisticados.

Metodos de deteccao

Como vimos anteriormente, os virus mais antigos deixavam rastros que possibilitavam sua descoberta:

Sintomas:

Demora maior na execucao de um programa. O sistema fica mais lento como um todo.

Aumento no tamanho dos programas.

Alteracao na data de criacao do programa. Quando o virus infecta, o programa aparece uma data de criacao recente.

No caso de virus de disco, e' possivel que alguns arquivos do disquete pura e simplesmente desaparecam.

Igualmente o aparecimento de mensagem acusando Bad Cluster em todos os disquetes usados (nao confundir com o que acontece com um disquete de 360k formatado por engano para 1.2 de capacidade). Nos tempos do virus Ping-pong, essa

era uma dica de infeccao.

Disquete funciona em PC-XT mas nao funciona em um PC-AT.

Antivirus alerta para modificacao em seu arquivo (os novos programas antivirus nao funcionam quando sao modificados pela infeccao de um virus). Nao se deve utiliza-los mesmo quando possivel se houver virus na memoria, pois isso infecta todos os arquivos que forem examinados.

Utilizacao de ferramentas como Norton Utilities ou PCTOOLS para visualizacao do setor de Boot mostram modificacoes (so' para quem sabe a diferenca).

Programa Windows deixa de funcionar ou congela repetidamente.

Para se "limpar" um virus

O mais simples e' o uso de um antivirus, como o Scan, NAV, Thunderbyte, ou F-Prot. Cada um destes tem sua propria forma de utilizacao.

Atualmente o Thunderbyte e o F-Prot estao ganhando uma otima reputacao, embora o Scan ainda seja capaz de proezas na limpeza de virus polimorficos, por exemplo.

O Norton Antivirus possui em seu pacote um programa denominado Vacina, que, como o VShield (da mesma firma que fabrica o Scan) vigia para a entrada de virus e e' recomendavel. O NAV em si tem os seus defensores, mas alguns o consideram um desperdicio de espaco na Winchester.

O F-Prot possui um banco de dados contendo descricoes de virus de computador ja' analisados por eles. A firma edita tambem um boletim sobre virus, disponivel em ftp site e em www, com boas descricoes sobre novos problemas causados por novos tipos de virus.

O Scan da MCafee alterou recentemente o formato original de programa. Alguns o consideram mais vulneravel a acao de virus anti-virus (os chamados retro-virus).

Ate' a versao 6.2 do DOS existia um antivirus da Central Point junto com o pacote. Gerou um rebulico pela quantidade de falso-positivos (dava alarmes falsos) que gerava, quando usado em conjunto com outros antivirus. Sua eficacia era igualmente reduzida pelo fato de que nao e' facil de atualizar. Novos tipos de virus passariam indetectaveis.

Precaucoes:

Antes de qualquer tentativa de se limpar um micro ou um disco deve-se dar um BOOT com um disquete limpo de virus. Este disquete, se nao existir, deve ser feito em algum outro micro onde o virus nao apareceu, atraves do comando SYS. Apos a copia do sistema operacional para o disquete, copia-se o antivirus para o disquete e coloca-se a etiqueta de protecao. Desliga-se o micro e liga-o novamente como o

novo disquete de sistema, (devidamente protegido contra gravacao atraves da etiqueta) no drive A:.

Sabendo-se que determinado disquete contem virus de disco, a forma correta de se limpa-lo sem recorrer a antivirus e' atraves do comando SYS do DOS. E' necessario que o disquete tenha espaco suficiente para que o comando funcione, portanto se usa o PCTOOLS ou algum outro programa copiador de arquivos para copiar os arquivos antes de executar o comando SYS A: ou SYS B:. O ideal e' formatar o disquete.

No caso do disco rigido infectado com virus de disco, e' necessario garantir o salvamento ou o back-up dos dados mais importantes, como:

arquivos de configuracao:
autoexec.bat, config.sys, win.ini, etc

arquivos de dados:
aqueles com os quais voce trabalha desde o ultimo back-up.

Em seguida, usar o comando MIRROR para fazer uma copia do boot sector do disco em disquete (que ficara' infectado, mas podera' ser limpo depois com mais facilidade). Feito isso, pode-se apartir do prompt do DOS no drive C: digitar:

```
C:\> \dos\fdisk /mbr
```

Imediatamente se desliga o micro, para evitar reinfeccao. Essa tecnica funciona em muitos casos, mas o inteligente e' executa-la tendo inicializado o micro com um disquete limpo de virus no drive a: (nao existe nada melhor).

No caso de micro contaminado por virus de arquivo polimorfico(NATAS ou FREDDY), o ideal e' a re-instalacao de todos os arquivos infectados, comecando pelo command.com. Arquivos texto poderao ser salvos.

Algumas dicas para o SCAN:

Pode-se pesquisar muitos disquetes de uma so' vez com a seguinte linha de comando:

```
C:\> scan a: /many
```

Para se evitar o tempo que o antivirus perde checando a memoria:

```
C:\> scan a: /nomem
```

Para se ter as instrucoes do Scan e do Clean em portugues existe um arquivo de extensao .msg, disponivel na maioria dos sitios que possuem antivirus. E' so' renomear o arquivo para MCAFEE.MSG e automaticamente o scan adota as mensagens daquela linguagem.

EX:

C:\> ren spanish.msg mcafee.msg

As ultimas versoes do Scan (2.3) tem a lista de virus e o antivirus Clean incorporado.

ex: scan c: /clean

Automaticamente limpa os arquivos infectados

ex: scan /vlist

Exibe uma lista dos virus que esse antivirus detecta (e/ou limpa).

Como funciona um programa antivirus:

Pouca gente que trabalha com isso desconhece. Sao tres as principais formas de se detectar a acao de um virus num sistema atraves do programa antivirus.

1) Vigiando a memoria do micro para acao de qualquer novo programa (quando o virus e' residente, ele ocupa espaco na memoria e pode ser rastreado atraves de programas como o CHKDSK ou MEM /c) ou outros sinais de infeccao.

2) Mantendo um arquivo com as caracteristicas do(s) arquivos antes da infeccao. Assim, como se fosse um policial, ele ele examina o CRC, a data de criacao do arquivo, o tamanho e outras caracteristicas cuja alteracao denunciaria acao indevida.

3) Abrindo cada um dos arquivos passiveis de infeccao e examinando o codigo do programa. Lembrar que o virus e' um programa de computador que se copia sem intervencao humana para outro programa ou boot sector. Um programa e' composto de as vezes milhares de instrucoes em linguagem de baixo nivel.
      O que o programa anti-virus faz e' ler esse "texto" dos arquivos executaveis (de extensao .COM, .EXE ou .OVL, entre outros) e procurar por uma linha de codigo caracteristica de virus de computador. O programa, ao encontrar uma semelhanca entre o codigo do virus e a linha de codigo que ele tem armazenada na memoria como pertencente a um virus, aciona a mensagem de alerta para o usuario.

Observacao: Alarmes falsos -   Algumas vezes quando o antivirus nao foi bem testado, o programa pode classificar outro programa como infectado, so porque ele encontrou essa parte do codigo, sem que exista nenhum virus no computador (a isso se chama o falso alarme). Esse tipo de busca e' tambem feito na memoria do micro, algumas vezes tambem com o mesmo efeito, sendo famoso o antivirus disponivel com a versao 6.2 do MSDOS. Se fosse usado junto com o antivirus SCAN versao 108 (nao tenho certeza), este emitia a mensagem de que o virus "Protector" estava

ativo na memoria (quando na verdade o antivirus e'
que estava).

Para se estudar um virus:

Para as almas corajosas que querem, por uma razao ou outra colecionar virus para estudo (atitude que aprovo, desde que o fim seja o de aprender alguma forma de se livrar deles de forma mais facil), aqui vao algumas dicas.

Em primeiro lugar, nunca estudar o virus em um micro contendo arquivos de outra pessoa com dados valiosos que possam ser perdidos. Se for usar o seu micro, certifique-se de que tem todos os arquivos back-up guardados e faca novo BACK-UP antes do inicio do trabalho.

Segundo lugar. Tenha o virus copiado para um disquete. Isso e' feito atraves da copia do arquivo infectado para um disquete. No caso de virus de disco, formatando um disquete (com sistema operacional, usando format a: /s na linha de comando).

Terceiro lugar. Tenha um disquete de Boot, limpo de virus a mao. De preferencia dois, todos com etiqueta.

Quarto: modifique o autoexec.bat no disquete, adicionando o comando subst da seguinte maneira:

Ex:

```
   subst c: a:
   subst b: a:
   subst qualquer outro drive   a:
```

Obs: Em teoria isto vaiimpedir o virus de se propagar para o drive C:, mas o melhor ainda e' desligar a Winchester mexendo na configuracao da BIOS ou via desligamento da placa da winchester.

Feitas essas preparacoes, comeca-se a testar o virus. O ideal e' ter um arquivo de isca, com um codigo simple como esse:

```
{programa retirado da revista Virus Report - nr 4 pg 4 }
org 100h
code segment
assume cs:code, ds:code
programa proc
inicio:
   mov ah, 4Ch
   mov al, 0h
   int 21h
programa endp
code ends
end inicio
```

A ideia e' ter um programa cujo codigo nao confunda na hora de examinar. Na verdade, o programa poderia ser bem menor. So' que alguns virus se recusam a infectar programas com menos de 500 bytes. Compilar com o MASM ou TASM.

Havendo tal programa que chamarei de isca, deve-se

renomea-lo para isca.xxx antes do inicio das experiencias.
Para averiguar o comportamento do virus desenvolvi o
seguinte metodo:

1) Antes de ativar o programa infectado

Digitar;

```
dir isc*.* >> teste.doc
copy isca.xxx isca1.com
arquivo          <------------  aciona-se o arquivo virotico
echo "arquivo virotico ativado" >> teste.doc
  ^
  I
```

(Comando para inserir essa linha no arquivo de registro sem
editor de texto)

2) Uma vez o arquivo ativado (o virus provavelmente na
memoria)

Digitar:

```
dir isc*.* >> teste.doc
isca1
echo "isca1.com ativado" >> teste.doc
dir isc*.* >> teste.doc
```

3) realizar novo boot para tirar o virus da memoria

Digitar:

```
echo "situacao apos boot" >> teste.doc
dir isc*.* >> teste
```

Podem ser estudados:

- O aumento do arquivo apos a infeccao
- As diferencas na quantidade de memoria livre existen-
te apos ativacao (usando o CHKDSK e o MEM)
- O tipo de arquivos que infecta e se tem um tempo
de incubacao (tempo durante o qual nada acontece).
- Colocar varios arquivos juntos de uma so' vez,
para se determinar se e' fast-infector.
- Pode ser considerado "Stealth" se conseguir
esconder sua presenca.

Obs: Nao se deve em hipotese alguma executar o Debug com o
virus na memoria do micro.

Obs2: O virus pode ser considerado Stealth (furtivo) se
as alteracoes no arquivo ficarem visiveis com um boot
feito com disquete limpo de virus (no caso de um que
ataque arquivos).

Os virus de Boot sao estudados dando-se o boot com um
disquete infectado com o mesmo. Usar-se o comando SYS do
DOS para se implantar o sistema operacional no disquete
infectado apagara' o virus no disquete.

Exemplo de descricao de um virus que espalhou muita
destruicao, na Universidade de Sao Paulo (e outros
lugares, sem duvida)

Texto distribuido junto com o programa antivirus anti-brazil virus,
programa de autoria do Prof. Raul Weber
Instituto de Informatica - UFRGS - Brazil

Caracteristicas do "Brasil virus!"

A analise abaixo e' baseada em uma amostra do virus em um disquete de 360k.
Este setor foi enviado por Joseph Max Cohenca, da USP.

1. O virus nao e' detectado por nenhum anti-virus atualmente disponivel
ate' a date de 5 de outubro de 1992. Mais especificamente, o F-Prot 2.05
nao detecta nada, tanto em modo "normal" quanto em modo 'heuristico".
O scan 95b detecta um "Generic Boot Infector", mas isto e' simplesmente
um aviso de que o SCAN nao descobriu no setor de boot o codigo normal
de um disquete DOS. Se isto e' realmente um virus ou algum sistema
operacional "clonado" do DOS, o SCAN nao sabe. Por falta de
informacao a respeito, o CLEAN nao consegue restaurar o disquete.

2. O virus e' um virus de bootstrap, e parece ser inedito, ou seja, ou e'
realmente um virus brasileiro, ou uma copia muito modificada de um virus
ja' existente (como Stoned, Michelangelo ou Disk Killer).

3. O virus usa tres setores do disco (ou disquete). O primeiro setor, que
substitui o boot em disquetes ou o master boot de discos rigidos, contem
o codigo da ativacao inicial do virus, que e' executado quando se liga a
maquina ou se reinicializa ela (por reset ou Ctl-Alt-Del). O segundo setor
contem o codigo do virus que se torna residente, e que e' responsavel
pela propagacao e ataque do virus. No terceiro setor o virus guarda o
setor de boot original.

4. Em discos rigidos, o virus usa para os seus tres setores os setores 1, 2
e 3, do cilindro zero, cabeca zero. (Obs: nestes discos, o setor 1 e' o
masterboot, que contem a tabela de particao). Para eliminar o virus, basta
copiar o setor 3 (a copia do master boot original) de volta para o setor 1.

5. Em disquetes de 360k, o virus usa os setores 0, 10 e 11 (numeracao DOS;
isto significa set.1, cil.0, tr.0 (boot), set 2, cil.0, tr.1 (setor 10) e
set.3, cil.0, cab.1 (setor 11). Os setores 10 e 11 sao os setores finais
do diretorio raiz, e o virus pode causar problemas se existirem muitos
arquivos no diretorio raiz. Para eliminar o virus e restaurar o disquete,
basta copiar o setor 11 para o setor 0.

6. O virus tem a capacidade de infectar outros disquetes (720k, 1.2M e 1.44M),
localizando-se sempre nos dois ultimos setores do diretorio raiz, que tem
baixa probabilidade de serem ocupados pelo DOS.

7. O virus testa sua presenca atraves dos enderecos 01A8 e 01A9 (em hexa)
do setor de boot. Se estes dois bytes forem CF CF, o virus assume que ja'
infectou o disco. Se nao, o virus procede 'a infeccao.

8. O virus, durante sua carga (na inicializacao do sistema), intercepta
unicamente o vetor 13H da tabela de interrupcao do DOS. Esta entrada
realiza os servicos do BIOS de acesso a discos e disquetes.

9. O virus usa tecnicas de invisibilidade (Stealth) para impedir sua deteccao. Qualquer tentativa de leitura do setor de boot e' interceptada pelo virus, que devolve o setor original. Assim, para uma analise ser efetiva, o virus nao deve estar residente na memoria.

10. Ao realizar o seu ataque, o virus escreve "Brasil virus!" na posicao atual do cursor na tela. Este texto ("Brasil virus!") esta' criptografado e nao pode ser detectado por um programa editor de disco. Obs: Brasil esta' escrito com "s" e nao "z".

11. O virus somente infecta discos rigidos (na hora da carga do sistema) e disquetes no driver A:. Disquetes no driver B: nao sao infectados. Disquetes sao infectados ao realizar-se operacoes de leitura sobre os mesmos. Obs: um simples comando de "DIR" e' suficiente para infectar um disquete.

Os seguintes dados sao preliminares e necessitam de maior analise:

1. Para realizar o ataque, o virus conta tempo apos a infeccao do disco rigido. Aparentemente, passando-se 120 horas de uso do computador apos a primeira infeccao, o virus escreve a mensagem "Brasil virus!" na posicao atual do cursor, apaga as primeiras trilhas do disco rigido e "congela" o computador.

Um programa especifico para detectar e eliminar o "Brasil virus" ja' foi desenvolvida pelo Instituto de Informatica da UFRGS e esta' disponivel por ftp anonimo na maquina caracol.inf.ufrgs.br (143.54.2.99), diretorio pub/virus/pc, arquivo antibr2.zip.

Porque os virus sao escritos:

O chamado virus de computador e' um software que sempre capta atencao e estimula a curiosidade. Esta pergunta foi feita na convencao de Hackers e fabricantes de virus na Argentina. A primeira resposta foi:

- Because it's fun. (por diversao, entretenimento)

Outras respostas:

- Para estudar as possibilidades relativas ao estudo de vida artificial (de acordo com a frase de Stephen Hawkind "Os virus de computador sao a primeira forma de vida feita pelo homem"). Esta proposta e' seguida por varios cientistas, incluindo um que pos a disposicao seu virus (inofensivo) para aqueles que estivessem interessados. Existe uma revista eletronica dedicada a isto, chamada Artificial Life e varios livros sobre o assunto. Em suma algo serio.

- Para descobrir se sao capazes de fazer isso ou para mostrarem para os colegas do que sao capazes de fazer com um micro. Testar seus conhecimentos de computacao.

- Por frustracao ou desejo de vinganca. Muitos autores

de virus sao adolescentes. Um jovem (inconformado com o fato de que o pai nao esta' afim de comprar aquele kit de multimidia para o seu micro), usa o que sabe para ...
* Esta hipotese e' pura imaginacao. Mas a vontade de sublimar uma raiva atraves de atos de vandalismo existe, como demonstram os pichadores e quebradores de telefones.

- Curiosidade. Algo muito forte, mesmo para aqueles que tem pouco conhecimento de informatica. Uma das melhores formas de se aprender sobre virus e' "criando" um.

- Para conseguir acesso a BBSes de virus. Existem BBSes que possuem bibliotecas de virus e codigos fontes como a Viegas BBS (agora desativada) e outras nos EUA e em outros paises. O usuario podia ter acesso a colecao de virus se fornecesse um novo. Muitos criavam ou modifi-
-cavam virus ja' existentes p. ter esse acesso (alias dois tercos dos virus ja' registrados sao resultado desse intento, sendo muitos considerados fracos ou pouco sofisticados, comparados com os originais).

- Para punir aqueles que copiam programas de computador sem pagar direitos autorais.

- Para conseguir fama.

- Fins militares. Falou-se sobre isso na guerra do golfo, para esconder o uso de uma outra arma de "atrapalhamento" do sistema de computadores do inimigo. Ainda assim, os virus p. uso militar sao uma possibilidade.

etc, etc

Minha opiniao pessoal e' que as pessoas se interessam por virus de computadores da mesma forma que curtem assistir filmes de guerra e colecionam armas de fogo ou facas.
O fato de que a pessoa coleciona virus de computador ou cria novos especimes nao indica uma vontade de distribuir seus "rebentos" para o publico em geral.

Virus benignos:

Existem. Um deles e' o KOH, criado por King of Hearts, um hacker mexicano. Ele e' um virus que criptografa tudo, de acordo com uma senha escolhida pelo usuario. Desenvolvido com o algoritmo IDEA, e' teoricamente dificil de ser "quebrado". O utilizador desse virus pode "pedir" ao virus para nao infectar disquetes ou disco rigidos e controlar sua acao, portanto. Usa tecnicas "stealth" e e' invisivel portanto a antivirus, podendo mesmo ajudar a evitar alguns tipos de virus.
Outro, compacta, a semelhanca do programa PKLITE, todo e qualquer arquivo executavel que "infecta". O unico virus que "reduz" o espaco fisico que "ocupa". Sem prejudicar os programas que compacta.

Emuladores de virus

Sao programas que simulam a acao de virus de computador, para treinamento ou diversao (a custa dos outros). Existe um, antigo, que faz aparecer umas aranhas na tela que "comem" todas as letras do texto digitado. Outro exibe mensagens de erro, com os seguintes dizeres:

1- Erro tal. Sua Winchester esta' cheia de agua.
2- Barulho de Winchester "inundada" aparece no alto-falante do micro.
3- O sistema operacional avisa que vai centrifugar o disco rigido para tirar a agua. Barulho de centrifugacao no alto-falante do micro.
4- Volta o sistema ao normal.

Durante esse tempo todo, nada aconteceu com o seu micro. O teclado ficou travado, mas nenhum arquivo foi deletado, nem mudado de lugar. Mas quem nao conhece o dito fica em panico, e se e' o usuario "TAO" (aquele que aperta bo"TAO" de reset com a ideia de que vai ganhar presente depois), e' capaz de desistir de aprender computacao.

Mais util e' o Virsim2, um emulador de virus feito especialmente para treinar gente no combate a antivirus. O programa produz arquivos inofensivos (que sao detectados como se fossem infectados por diferentes tipos de virus, ver sessao sobre o funcionamento do Scan). Tambem e' capaz de "infectar" um disquete com um boot virotico (que nao infecta o disco rigido ou outros disquetes) ou simular o efeito de um virus na memoria. A instalacao do programa e' sofisticada, com uma voz (em ingles) explicando o que o programa esta' fazendo no momento, e isso funciona sem placa sound-blaster.

Engracado e' que em algumas firmas onde este programa foi usado constatou-se que nenhum dos arquivos ficticios infectados foi encontrado pelos funcionarios. Constatou-se uma apatia total pelo uso de programas anti-virus (ja' que nao havia virus, nao havia medo de virus, entao nao havia uso dos programas anti-virus instalados).

Revistas e fontes de informacoes para estudiosos de virus:

Existem. De um lado a Virus Bulletin, publicada na Inglaterra uma das maiores autoridades no assunto, mas e' paga (75 Libras) anuais, creio. Existe o Virus Bulletin da Datafellows, que e' disponivel via ftp e WWW. Faz parte do lancamento de cada nova versao do antivirus F-Prot. Contem bastante material interessante. O unico problema e' que a enfase sao de virus Nordicos, o que e' compreensivel, ja' que o programa vem de la' (por sinal e' bastante bom e atualizado regularmente). A revista argentina Virus Report tambem e' uma excelente fonte de informacao sobre tudo o que diz respeito a virus e seguranca eletronica. E' a revista dos hackers argentinos e patrocinou recentemente um encontro internacional, do qual participei com uma palestra sobre ensino a distancia, trabalho feito pela ESCOLA DO FUTURO.
Em Buenos Aires haviam mais duas ou tres revistas sobre virus de computador em formato eletronico, mas nao tive chance de conseguir nenhuma copia.

Atraves da Internet e' possivel se conseguir, no sitio ftp do Cert, os arquivos Factory.zip, Virus.101-4, e o VSUM fontes quase basicas de informacoes sobre virus. O arquivo Factory.zip delinea a mecanica de funcionamento da fabrica de virus na Bulgaria, pais responsavel por abrigar programadores que muito contribuiram para os problemas do mundo ocidental ate' bem depois da queda do muro de Berlin. Lendo esse arquivo sabemos a origem do virus DIR-II e de outros.
Existem varias revistas que ensinam tecnicas de fabricacao de virus e manuseio. As mais conhecidas sao a 40hex, a NUKE, e a CriPT, mas se nao me engano esporadicamente pode-se encontrar artigos sobre essas tecnicas na Phrack, NIA e CUD. Existe tambem um arquivo denominado Hack-report, com um relato de quais sao os ultimos cavalos de troia e bombas-logicas que estao sendo distribuidos ate' a publicacao do artigo. Uma das primeiras revistas sobre o assunto foi a CPI - Corrupted Programming International, que tinha ate' mesmo exemplos de listagem em Assembly, Turbo Pascal, Basic e Batch File Programming, pra mostrar que qualquer linguagem pode produzir estas monstruosidades. Alguem escreveu um livro aproveitando isso, aqui no Brasil, mas acho que nem em sebo se encontra.
A revista 2600 e a HACK-TIC tambem as vezes publicam artigos sobre isso, so' que em papel.
Os grupos de discussao na Internet V-alert e Comp.virus sao bastante uteis p. alertas sobre novos virus e discussao de outros recentes ou nao. Seu FAQ (Frequent Answered Questions) texto e' uma excelente fonte p. quem nao conhece muito sobre o assunto. Vasselin Bontchev, seu moderador e' uma das maiores autoridades no assunto.
Ouvi dizer que existem um grupo de discussao IRC que trocam dicas on-line sobre fabricacao de virus na Internet, mas nao conheco maiores detalhes.

Nomenclatura de virus:

Nao existe uma convencao sobre o assunto. Enquanto os fabricantes de virus costumam trocar dicas e ideias, os fabricantes de antivirus normalmente se fecham em si, cada qual defendendo o seu mercado. O que e' Athenas para o Scan da Mcafee Software, e' Trojector para o F-Prot do Friedriek Skulasson. O maior documento, e em formato hipertexto, sobre virus, e' o VSUM, produzido pela Patricia Hoffman. Como parece que ela recebe dinheiro da Mcafee, ou porque sua descricao e' duvidosa (nao sei o porque na verdade), o fato e' que este documento nao e' aceito pela comunidade de pesquisadores anti-virus. Pelo menos nao o e' na sua totalidade. Existem vozes discordantes.

Num de seus boletins, a firma que produz o F-Prot conta tudo sobre como elabora a nomenclatura de seus virus, mas se trata de uma leitura chata. O "nosso" virus Brazil nao aparece na lista deles nem do Scan como tal, por exemplo. Ja' um virus chamado Xuxa, muito raro (parece que foi escrito so' p. fins de divulgacao) e' chamado como tal.

As vezes, o virus e' nomeado por se tratar de uma modificacao de outro ja' existente ou pelo programa que o produziu (como acontece com os virus produzidos com a ajuda do VCL - ver os kits de producao de virus). As vezes o virus contem um sinal (ele tem que saber como identificar um arquivo virotico, p. nao infectar repetidas vezes o mesmo

arquivo) e esta caracteristica "batiza" o virus.

Programas "falsos":

Algumas vezes, aparecem "ultimas versoes" ou versoes "desprote-
gidas" de softwares muito utilizados. O sujeito copia, usa em
casa, e .. descobre que o software e' na verdade um programa
de formatacao fisica de Winchester disfarcado de outra coisa.
Esse e' o tipo de virus classificado como "cavalo de troia" ou
"bomba-logica".
      Na Viegas BBS havia alguns programas do genero, inclu-
-sive um "Norton Virus Detector", antecipando em alguns anos
a producao do programa antivirus do Norton. Esse tipo de fal-
sificacao aconteceu muito com o Scan, o Pkzip e acho que ate'
com o Arj. O programa na verdade instalava um virus ou fazia
alguma coisa ruim com os dados da winchester.
      Um caso que deu muito o que falar foi o do "AIDS-virus".
Era um programa com informacoes sobre a AIDS. O sujeito respon-
-dia algumas perguntas, recebia alguma informacao geral sobre
o virus (biologico) e tudo bem. So' depois descobria que todos
os nomes, todas as extensoes de arquivo, tudo o que estava na
 Winchester havia sido alterado. A seguinte mensagem aparecia:

 "It is time to pay for your software lease from PC Cyborg
 Corporation. Complete the INVOICE and attach payment for the lease
 option of your choice.If you don't use the printed INVOICE, then be
 sure to refer to the important reference numbers below in all
 correspondence.

  In return you will recieve:
    - a renewal software package with easy to follow,
      complete instructions;
    - an automatic, self installing diskette
      that anyone can apply in minutes."

      Isso podia ser uma propaganda contra software pirata,
mas na verdade o software foi distribuido gratuitamente como
brinde numa convencao internacional sobre AIDS e tambem numa
revista de informatica tipo PC-Qualquer coisa.
      Como ja' foi dito acima, a unica forma de prevencao
contra esse tipo de programa e' um software chamado CHK4BOMB,
disponivel no subdiretorio virus de qualquer "mirror" do
Simtel20. Ainda assim nada realmente e' capaz de garantir que
um programa e' ou nao um "cavalo-de-troia".

Laboratorios de fabricacao de virus:

Existem programas feitos especificamente com o proposito de
auxiliar iniciantes na arte de fabricar virus sofisticados.
Sao os "Virus Construction Tools". Existem bibliotecas de
rotinas prontas que podem tornar um virus simples polimor-
fico (mais dificil de detectar) sem grande dificuldade p.
o programador. E programas que fazem o servico completo

ao gosto do "inteligente" que quiser construir seu proprio "monstro".

O primeiro foi o GENVIR, construido e distribuido na Franca. Lancado como uma especie de Shareware, e' cheio de menus, mas na hora de produzir o virus ele para. Para receber uma copia que realmente faca o trabalho, a pessoa deveria enviar 120 francos para um endereco na Franca.

Um grupo alemao o "Verband Deutscher Virenliebhaber" escreveu o VCS (Virus Construction Set). Esse incorpora um texto escolhido pelo usuario num virus simples, que apos se reproduzir um numero x de vezes, deleta os arquivos de configuracao, como AUTOEXEC.BAT e CONFIG.SYS.

Outros kits mais "completos" e "sofisticados" sao o VCL (Virus Construction Laboratory), o PS-MPC (Phalcon/ Skism - Mass Produced Code Generator), o IVP (Instant Virus Production Kit) e o G2 (G ao quadrado). Alguns chegam a produzir virus com caracteristicas avancadas, como criptografacao e otimizacao de codigo virotico(!). Como os fabricantes de antivirus tambem se mantem atualizados, os programas antivirus sao atualizados de forma a detectar os virus produzidos por esses laboratorio.

Algumas crendices:

Contaminacao por Modem de computador:

Nao existe. Pode-se conseguir um numa BBS ou com um amigo atraves da copia de um programa infectado, mas e' tecnicamente impossivel um micro infectar outro atraves do uso de modem.

Contaminacao por cima da etiqueta de protecao:

Tambem impossivel. O que pode ter acontecido e' a infeccao ter sido descoberta depois da colocacao da etiqueta, coisa que acontece com virus "stealth". Essa trava impede a gravacao no disquete e isso funciona a nivel de hardware, nao de software.

E' necessario formatar todos os disquetes para se livrar do virus XXXX---
---

Nem sempre. Tudo depende de se ter ou nao o "disquete de sistema limpo de virus". Com ele e' possivel so' apagar os programas infectados e evitar esse trabalho. De acordo com a minha experiencia e' possivel usar uma ferramenta como o PCTOOLS ou o XTREE para "salvar" os arquivos de dados, sem aumentar a transmissao. Em alguns casos pode ser mais facil formatar e re-instalar tudo do que fazer a limpeza, mas nem sempre.

So' software pirata contem virus

Nem sempre. O Michelangelo foi distribuido pela primeira vez dentro de 20.000 disquetes distribuidos por uma firma de

computacao a seus usuarios. O computador que fazia as copias estava infectado. Houve tambem o caso de um programa famoso de Desktop Publishing cujos disquetes-matriz foram infectados na casa do sujeito encarregado de dar uma ultima olhada, resultando que toda a producao foi infectada.

Calendario de Virus:

Essa e' uma favorita da imprensa. Nao se fazem mais as reportagens sobre supersticao na Sexta-feira 13 (como antigamente). Mas com certeza se fazem reportagem sobre o virus Sexta-Feira 13 e o problema dos virus que tem dia certo para ativar.
A maior incidencia de virus no Brasil, de acordo com bate-papos com gente que faz acessoria de informatica sao de virus como o Stoned, o Michelangelo, o Jerusalem, o Athenas (trojector) e ultimamente o Freddy. Aqui e ali ocorrem surtos de alguns virus novos, como o GV-MG e o Daniela.
Desses, so' um ou dois tem ativacao por dia do ano. O Michelangelo, 6 de Marco, e o Sexta-Feira 13. O pro--blema e' que se a pessoa for esperta e fizer uma check-up regular no micro, com qualquer programa como o Vshield ou Vacina (ate' mesmo o MSAV do Dos 6.2 e' o suficiente para isso), ira' descobrir o intruso.
Para se ter uma ideia, existem versoes modificadas tanto do sexta-feira 13 como do Miguelangelo, que detectam quando o dono do micro desligou para "evitar" o dia fatidico. Funcionam no dia ou na semana seguinte.

Virus "Good Times"

Esta e' aconteceu na Internet, mas nao duvido que tenha acontecido tambem em BBSes por ai' afora. Era um aviso sobre um virus que apagava tudo no disco rigido, veicu-lado em correio eletronico. Funcionava como uma daquelas correntes da felicidade. O sujeito recebia o aviso e re-enviava para todo mundo que conhecia, e esses tambem re-enviavam.
O efeito do virus foi "torrar" a paciencia e ajudar a encher o correio eletronico (em alguns servicos de BBS paga-se por quantidade de correspondencia recebida) de muita gente. Depois veio uma segunda onda, a daqueles que avisavam que o virus nao existia.

Bibliografia:

- The Bulgarian Factory (factory.zip) Vasselin Bontchev
- Revistas Eletronicas 40hex, NUKE, Phrack, LoD, CuD, CPI
- VSUM - Patricia Hoffman
- The Little Black Book of Computer Virus - Mark Ludwig
- Computer Viruses, Artificial Life & Evolution - idem
- 2600 Hacker Quaterly
- Hack-Tic
- Virus Bulletin - numeros 08, 09, 15 e 16

- Hacker Bulletin
- Coletantea de artigos Virus.101 - 104
- Aids Attack - artigo
- Virus Report - numero 4
- Conferencias da Reuniao de Hackers na Argentina.
- Conversas com varios amigos: R.E.K, M.E.V. e outros ratos

Enderecos e referencias para aqueles que decidirem se aventurar na rede:

AlDigest
alife@cognet.ucla.edu
ftp   polaris.cognet.ucla.edu

Alife
mxserner@ubik.demon.co.uk
ftp.informatik.uni-hamburg.de pub/virus/texts
ftp.demon.co.uk

40hex
ftp.eff.org

Phrack
ftp.eff.org
www.freeside.com

Varios artigos sobre virus, vsum, etc
Coast.cs.purdue.edu
rzsun2.informatik.uni-hamburg.de

Virus Bulletin - F-prot
ftp.datafellows.fi
www.datafellows.fi

Virus Report
(nao existe distribuicao no Brasil. O Fernando chegou a me propor
um lance nesse sentido, mas nada foi firmado. Quem se interessar,
escreva para: Fernando Bomsembiane
            Guemes 160 Ito 2
            Ramos Mejia (1704)
            Republica Argentina)

BBSes Argentinas (virus BBSes e outros lances)
 Nao sei o codigo de Buenos Aires, nao acessei nenhuma

 253-2098   Dinisyus2 ou Dionisyus2
 253-4389   Dinisius1 ou Dionisius1
 383-7480   Satanic Brain   Senha e' Chacal

ARTIGO EXTRAIDO DA REVISTA UXU N 144 - disponivel na ftp.eff.org
subdiretorio pub/Publications/CuD

2600
POB 752

Middle Island NY
11953

Absolutely the best hard copy hacker magazine. Articles range from phone company switching system programming to cellular hacking to defeating Simplex locks. Editor Emmanuel Goldstein is one of those rare editors that uses the freedom of the press to the utmost: always a step ahead of those that would like to see him jailed.

2600 also offers a video of Dutch hackers breaking into a military computer. Excerpts of this video were shown on "journalist" Geraldo Rivera's sensationalist TV show. The video is $10.00.

2600 operates a voice BBS (0700-751-2600 0.15/minute) which is open from 11 PM to 7 AM every day.

2600 holds meetings in many major US cities every first Friday of the month. See the current issue for listings.

Subscriptions (four issues) are $21.00 (US and Canada); $30.00 (foreign).

TAP
POB 20264
Louisville KY
40250-0264

TAP, or the Technical Assistance Program, has been in (erratic) publication since 1973. It was originally titled Youth International Party Line (YIPL) after it's founders Yippie Abbie Hoffman and phone phreak Al Bell. TAP published articles on scams, concentrating particularly on phone fraud. TAP stopped publishing for a while when then-publisher Thomas Edison's house was set on fire and computer stolen. TAP was then resurrected several times before it came to rest with Predat0r in 1990.

Each issue is $2.00, but send a letter before any money - issues have come out erratically.

Intertek
13 Daffodil Lane
San Carlos CA
94070

The journal of Technology and Society. Past issues have included articles on virtual communities (MUDs, IRC and such), Internet culture, and hacking.

Subscriptions are $14.00 four issues.

Hack-Tic
PB 22953, 1100 DL
Amsterdam
Netherlands

Hack-Tic is the Dutch equivalent of 2600 Magazine. Mostly written in Dutch, HT contains articles on phone phreaking and hacking in Europe (in the Netherlands it isn't a crime. Yet.).

Hack-Tic also sells the Demon Dialer rainbow box kit for $250.

They also sponsor the Galactic Hacker's Party, a worldwide gathering of phreaks, cyberpunks, and hackers.

Each issue of Hack-Tic is $2.50.

Chaos Computer Club
Schwenckestrasse 85
W-2000 Hamburg 20
Germany

The CCC is one of the most notorious hacker gangs in the world, and claim responsibility for all sorts of break-ins into the US Government's computer systems. One of their supposed members was the villain in Cliff Stoll's The Cuckoo's Egg.

They sell their secrets in Die Hacker Bibel Volumes 1, 2, and 3, and Das Chaos Computer Buch, plus other software programs. Catalog is free, but it is written in German, so good luck. Associating with these folks will probably land you on a government watch list.

Chaos Computer Club has two Internet archives:
ftp.eff.org pub/cud/ccc
ftp.titania.mathematik.uni-ulm.de /info/CCC

LOD Communications
603 W.13 #1A-278
Austin TX
78701
lodcom@mindvox.phantom.com

Sells the archives of "golden age of hacking" message boards - boards like OSUNY, Plovernet, 8BBS, Black Ice Private, and the Phoenix Project. Write for prices; available in Mac/IBM/Amiga formats.

Electronic Zines/Publications/Newsletters

Activist Times, Inc
gzero@tronsbox.xei.com
PO Box 2501
Bloomfield NJ
07003

Hacking, political viewpoints, anarchy, news. ATI is a lot smaller than most CU zines, but worth subscribing to.

Phrack
listserv@stormking.com

Phrack is the undisputed king of the electronic hacker magazines. Each huge issue (some are over 720K!) has detailed technical information on selected computer systems or phone equipment, a question and answer letters section, and articles on freedom and privacy in cyberspace. Phrack also has the Pro-Phile -an in-depth look at some of the most notorious hackers, and Phrack World News, a collection of newsclippings dealing with the computer underground.

Phrack is just to good to pass up - get it while it (and the editor and writers!) is still free.

Phantasy
iirg@world.std.com

Phantasy is the journal of the International Information Retrieval Guild, a hacking group with a few pirate ties. Similar to Phrack in content, but smaller.

Digital Free Press
dfp-req%underg@uunet.uu.net
     Irregularly published underground magazine.

Informatik
inform@doc.cc.utexas.edu
     Another superb hacker magazine. Informatik is very similar to Phrack, but with different information.

Telecom Digest
telecom-request@eecs.nwu.edu
     Daily digest covering all facets of the telecommunications industry, including breaking news and future plans of telecom companies. Highly recommended, but volume can be high - sometimes the digest generates two to three issues a day.

Security Digest
security-request@aim.rutgers.edu
     All topics of computer security are discussed on this list.

Telecom Privacy Digest
telecom-priv-request@pica.army.mil
     Digest devoted to privacy issues involving telecommunications (particularly CallerID, and similar services).

Ethics-L
listserv@marist.edu
     Ethics-L is a forum for the ethical use of computers, especially in an open environment such as a university.

Computer Underground Digest
tk0jut2@niu.bitnet
     The Computer Underground Digest, or CuD as it is called by its readers, is a weekly electronic news journal. It's beginnings stem back to early 1990, when Telecom Digest was inundated with posts about the recent Knight Lightning and Terminus indictments. Jim Thomas, a professor of sociology and criminology at Northern Illinois University, and Gordon Meyer, author of "The Social Organization of the Computer Underground," collected the excess posts and published them under the banner of CuD.
     The goal of CuD, according to its founders, is to provide a forum for discussion and debate of the computer telecommunications culture, with special emphasis on alternative groups that exist outside the conventional computer network community.
     CuD publishes:
     * Reasoned and thoughtful debates about economic, ethical, legal, and other issues related to the computer underground.
     * Verbatim printed newspaper or magazine articles containing relevant stories.
     * Public domain legal documents including affidavits,

indictments, and court records that pertain to the computer underground.
     * General discussion of news, problems, and other issues that contributors feel should be aired.
     * Unpublished academic pieces or research results.
     * Book reviews that address the social implications of computer technology
     * Announcements for meetings, conferences, etc.
(from the Computer Underground Digest FAQ).

EFFector Online
effnews-request@eff.org
     EFF news and recent trials, information, and such.

Virus-L Digest
kruw@cert.sei.cmu.edu
     Recent virus reports, analyzation of source code, critiques of anti-virus software.

Risks Forum
risks-request@csl.sri.com
     Funded by SRI (see below), Risks Forum discusses all aspects of public access and open-system computing.

Worldview/Der Weltanschauung
dfox@wixer.cactus.org
     News, tips and stories of the computer underground, telecom, and other information systems.

United Phreakers' Inc.
ftp.eff.org /pub/cud/upi
     Mostly a phreaker's rag, with info on PBXs, telecom services, telecom lingo, underground newsline, and bust news.
ccapuc@caticsuf.csufresno.edu
     CuD ripoff with different information. Includes CPSR releases.

Usenet
------
alt.hackers
     Not crackers, but people who like to do unconventional things with their computers. The real hackers.
alt.hackers.malicious
     People who like to destroy other people's information.
comp.society.cu-digest
     Usenet distribution point for Computer Underground Digest.
misc.security
     All sorts of security topics: computers, electronic locks, locksmithing, and so forth.
comp.org.eff.talk
     Discussion of EFF and projects.
alt.comp.acad-freedom
     Discussion of freedom of academic computing.
alt.dcom.telecom

Telecommunications talk. Pretty technical.

alt.dcom.isdn

ISDN services and possibilities are the talk here.

alt.radio.scanner

Newsgroup for scanner enthusiasts. Unconventional/illegal frequencies are sometimes posted here.

comp.risks

Similar to Risks Forum.

alt.society.ati

The Usenet distribution point for Activist Times Incorporated.

comp.security.misc

Anti-piracy tactics, bugs and holes in software.

FTP Sites

---

ftp.eff.org

Does this site have everything or what? Contains state computer crime laws, Computer Underground Digest archives, tons of hacker magazines, EFF news and announcements, guides to the Internet, and a lot more.

cert.sei.cmu.edu

Archives of the computer emergency response team.

Computer Underground Books

The Hacker Crackdown by Bruce Sterling

The Hacker Crackdown is cyberpunk author Bruce Sterling's first foray into non-fiction writing. Crackdown is an account of the government crackdown on the computer underground in the early 1990's. Includes a brief history of the telephone industry, events that led up to "Operation Sundevil," the Phrack/Bellsouth E911 fiasco, the trials that followed, and the formation of the Electronic Frontier Foundation. Highly recommended.

Cyberpunk by Katie Hafner and John Markoff

Three stories written by news reporters about computer hackers.

The first story is about Kevin Mitnick and friends' exploits.

The authors' dislike of Mitnick is obvious, describing in detail Mitnick's character flaws, and makes personal digs at him whenever possible.

The next story is about Pengo, the German hacker who offered to sell his (and his friends') talents to the Russians.

Finally, the last chapter tells the story of Robert T. Morris, author of the Internet Worm.

Although somewhat biased, Cyberpunk!, like The Cuckoo's Egg, is a must-read for those interested in hackers.

The Official Phreaker's Manual

This is the Bible of Phreakdom; includes terms and techniques (most outdated by now, but it gets the methods and possibilities across quite well). There's a bit of history thrown in - it contains the 1971 Esquire article about Capn

Crunch and his blue boxes. This manual brings back a lot of nostalgia, but I wouldn't use the tactics inside.

Available free on ftp.eff.org /pub/cud/misc.

Hackers by Stephen Levy

Hackers is the story of the true hackers - the geniuses responsible for the personal computer revolution.

The beginning of Hackers is about the first generation - students at MIT who formed a loose alliance and wrote amazingly clever programs on the facility's mainframes and minicomputers. The first generation were the ones that introduced the extremely anti-bureaucratic "Hacker Ethic" - the idea that computer should always be accessible, that artificial boundaries (including locked doors and closed buildings) should be overcome, and that "authority" should be mistrusted.

The second part is devoted to the second generation. These people were responsible for the birth of the personal computer, including Jobs and Wozniak, the Altair, and the Homebrew Computer Club. The second wave of hackers established the Do It Yourself attitude, and for the most part began the Computer Revolution.

The last part of the book is about the third generation of hackers. These were the software writers and programming geniuses, and the WarGames-era dark side hackers. The third generation was responsible for turning the PC from a hobbyist's toy to a household appliance.

The Anarchist's Guide to the BBS by Keith Wade

Describes in detail modems, protocols, and everything you need to start up your own anarchy BBS. Explains terms and techniques, excellent for beginners to the modem world.

The Hacker's Dictionary by Guy Steel, Jr

Terms and words used by programmers and true hackers. Media and security "experts" will be disappointed in this book, but those who find computers and computer history will find it entertaining.

The Cuckoo's Egg by Cliff Stoll

Cliff Stoll, an astrophysicist turned computer manager at Lawrence Berkeley Lab, narrates the true story of how he traced a 75 cent accounting error to a hacker who was breaking into the LBL system. The situation escalates as the hacker travels through the Internet, breaking into sensitive American computers and stealing military and R&D information to sell to the Russian. Stoll tracks the hacker through Berkeley's system, computer networks throughout the country, and the globe-spanning, tangled web of the phone networks.

This is one of the best books of high tech espionage, and a decent primer on Internet jargon. Highly recommended.

Computer Viruses: A High Tech Disease by Ralf Burger

Contains information on how viruses work and how they reproduce themselves.

Spectacular Computer Crimes by Buck Bloombecker

Mr. Bloombecker is the director for the National Center for Computer Crime Data, so you already know what he thinks about hackers. Spectacular Computer Crimes is a somewhat slanted collection of true stories on hackers, thieves, and assorted techno-troublemakers.

Approaching Zero by Paul Mungo and Bryan Clough

Yet another book on hackers by a journalist.

Narrative chronicles of the computer underground. Includes the deeds and antics of several legendary hackers, including Cap'n Crunch, Captain Zap, Fry Guy, Pengo, and virus writer Dark Avenger.

A good if somewhat basic overview of the alternative computer culture.

Little Black Book of Computer Viruses
American Eagle Publications, Inc
POB 41401
Tucson AZ
85717

Source code and description of popular viruses. For volume two, the author held a virus-writing contest, which was the subject of much controversy on the Internet.

American Eagle also publishes Computer Virus Developments Quarterly ($95 for a subscription).

==========

* Este arquivo veio da revista UXU-148, disponivel no ftp.eff.org
* subdiretorio pub/Pubications/CuD. O assunto sao substancias
* utilizadas por gente idosa. Quem leu Neuromancer ou a revista
* Wired tem um certo conhecimento desse tipo de substancia, os
* aceleradores de metabolismo cerebral. Nos EUA, a FDA se recusou
* a examinar esse tipo de remedio por nao acreditar que falta de
* memoria seja doenca. Nao existem dados o suficiente para se
* questionar os efeitos colaterais. Se o individuo usa, tem uma
* serie de efeitos positivos. Se para, a falta de memoria aparece
* para depois de algum tempo voltar ao normal. Mas como a Hacker
* Scene volta e meia discute a utilidade ou nao dos litros e litros
* de cafeina e substancias relacionadas para ficar acordado na frente
* da tela de um micro (Balzac, senao me engano morreu por intoxicacao
* provocada por excesso de consumo de cafe') vai ai o texto como
* curiosidade. Nao aconselho o consumo de qualquer substancia.

Smart Drugs

"Smart Drugs" are drugs that have been found to have beneficial mind enhancing effects, such as delaying aging, enhancing brain metabolism, improving memory, concentration, and problem solving techniques. Smart drugs are also called nootropics (Greek: mind acting). You will notice that many of these drugs were created and tested for people with nerve degenerative diseases, but they have been found to work for anyone.

Smart drugs are very popular among ravers and technophiles: these are the drugs that are necessary yo keep up with today's

information society.

Many smart drugs have a "bell-curve" dose response, that is - if you take too much of a drug, the opposite (bad memory, confusion) will happen. Smart drugs, for the most part, are virtually toxic free.

Smart drugs became popular after a loophole in the 1988 FDA policy (intended for AIDS drugs), which allowed for non-FDA approved drugs to be imported to the US for a limited time. As a result, drug export houses grew and the smart drug industry was born. Recently, the FDA has clamped down with import alerts, claiming they were trying to stamp out the "snake-oil salesmen." Many import houses were forced to shut down or close up shop. No doubt the FDA will also try to clamp down on the dietary supplements and vitamins industry. So proceed with smart drugs at your own risk.

NOTE: Do not use this book as medical advice. The following is presented for informational purposes only. Consult your doctor before you try ANY of the below substances.

NOTE: All dosage information has been removed from the original manuscript! I do not feel like getting sued just because some idiot tries some of these or mixes them with other medications.

Smart Drugs and Mind Nutrients

Vitacel 3-7

Benefits - Also known as Gerovital or GH-3/7, Vitacel 3-7 is a mixture of procaine, benzoic acid, and potassium metabisulfate (a powerful antioxidant). Vitacel has been tested to increase energy, memory, and treat depression.

Warnings - no known side effects.

Gingko Biloba

The gingko biloba is the oldest species of tree known, and it's leaves have been used by the Chinese as medicine for thousands of years.

Benefits - has been shown to improve cerebral circulation, an attentive, alert mind, and increases the body's production of adenosine triphosphate (an energy molecule). Ginkgo also enhances the ability to metabolize glucose. Gingko has been shown to act as an anti-oxidant.

Warnings and Side Effects - Ginkgo Biloba is safe, even in high quantities.

DMAE (Dimethylaminoethyl)

Benefits - DMAE increases physical energy, the ability to learn and remember, expands the life span of laboratory rats, and accelerates the synthesis of acetylcholine. DMAE produces a placid, moderate stimulant effect. Unlike coffee of amphetimines, this high won't cause insomnia or a quick letdown. Luckily, DMEA is regarded as a nutrition supplement, and can be easily purchased in the United States.

Warnings - Overdose may cause insomnia and tenseness of muscles. Manic depressives should steer clear of DMAE - it may augment depression.

Choline

Benefits - Choline is changed into acetylcholine when inside the body. Acetylcholine is the neurotransmitter used in memory functions, and studies have shown that taking choline improves memory for some.

Choline can be purchased in many health food stores, plus in a number of the catalogs below. Three forms of choline are common - choline chloride, choline bitartrate, and phosphatidyl choline. The best type to buy is phosphatidyl choline. PC repairs and maintains nerve and brain cells, aids in the metabolism of fat, and helps regulate cholesterol levels in the blood.

Warnings - Manic depressives should avoid taking choline supplements. Choline bitartrate and choline chloride can cause diarrhea.

Acetyl L-Carnitine

Benefits - Effects are similar to choline compounds, due to similar molecular structure. Acetyl L-Carnitine also inhibits the formation of lipofuscin (fatty deposits which are related to decreased mental faculties in the elderly). Acetyl L-Carnitine has been tested to increase alertness and attention span in Alzheimer patients.

Warnings - No studies have discovered any side effects.

Centrophenoxine

Benefits - Centrophenoxine removes lipofuscin deposits and repairs damaged synapses in the brian. Lipofuscin deposits are associated with aging and decreasing mental abilities. Centrophenoxine has also been shown to be an effective memory booster. Once in the body, centrophenoxine breaks down into DMAE and acts as a free radical scavenger.

Warnings - Should not be used by people who have very high blood pressure or are excitable. Side effects to centrophenoxine are scarce, but include insomnia, hyperexcitability, and depression. To allay these affects, lower dosages are recommended.

Deprenyl

Benefits - Deprenyl was originally developed for treating Parkinson's disease, but has been found to aid in fighting other problems, too. Deprenyl increases the brain's level of dopamine, a neurotransmitter that cause heightened emotional states, aggression, and raises one's libido. For these reasons, some treat Deprenyl as an aphrodisiac.

Warnings - can cause nausea in higher doses and death if taken with amphetamines.

Hydergine

Benefits - Hydergine is a type of ergot, a common rye fungus. When hydergine was being tested for other purposes in the late 1940's, many elderly subjects were reporting increased mental functions. Nowadays, hydergine is a very popular and inexpensive treatment for senility. It is the first drug to show strength against Alzheimer's disease.

Hydregine prevents damage to brain cells from insufficient oxygen, increases brain cell metabolism, and causes dendrites (branches of a nerve cell that receive information). Hydergine even appears to repair damage to brain cells.

Note - hydergine effectively synergizes with piracetam. If you plan on taking the two together, scale the dosage down on each.

Warnings - large doses may cause nausea or headaches. Strangely enough, an overdose of hydergine may cause amnesiac effects. If this should occur, just 1 '% ' osage.

Piracetam

Piracetam started the new pharmaceutical category of nootropics (Gr. "acting on the mind"). Piracetam is similar in composition to the amino acid pyroglutamate.

Benefits - Piracetam has been shown to enhance learning and memory. Piracetam promotes the flow of information between hemispheres of the brain. When these two side "talk" to each other, flashes of creativity (the eureka effect) often occur.

Piracetam uses up large amounts of acetylcholine, so a choline supplement will probably help in maximizing the effects.

Piracetam synergizes well with DMAE, centrophenoxine, and hydergine.

Warnings - Negative effects are very uncommon, but can include insomnia, nausea, and headaches. The toxicity level of piracetam is unknown.

Oxiracetam

Benefits - Oxiracetam is an analog of piracetam. Oxiracetam's potency is greater than piracetam and is more effective in memory improvement, concentration and stimulating alertness.

Warnings - Like piracetam, oxiracetam is very safe at all dosage levels.

DHEA

Benefits - Dehydroepiandrosterone is the most abundant steroid found in the body, and aids in fighting obesity, aging, and cancer.

Studies have linked low DHEA levels in the body with nerve degeneration. Furthermore, DHEA guards brain cells from Alzheimer's and other degenerative diseases.

Warnings - not much research identifies the side effects of long term use of DHEA.

Fipexide

Benefits - Fipexide improves short term memory and attention span. In addition to its cognitive enhancing effects, fipexide enhances the effects of dopamine (the neurotransmitter responsible for motivation and emotions), which can help lessen depression.

Warnings - No known side effects in recent medical literature.

Vasopressin

Vasopressin is a hormone released by the pituitary gland and

is used for imprinting new material into memory.

Benefits - Vasopressin improves memory retention and recall, concentration, and attention.

Certain drugs, such as LSD and cocaine, deplete the body's natural supply of vasopressin, so inhaling a spray of vasopressin can replenish the body. Also, since the release of vasopressin is impeded by alcohol and marijuana, a dose of bottled vasopressin will compensate.

Warnings - Can produce the following side effects: runny or itching nose, abdominal cramps, increased bowel movements. Shouldn't be used by people with high blood pressure.
NOTE: Vasopressin may be extremely difficult to obtain now -- it has been taken off the market in every country except for Spain.

Vincamine

Benefits - increases blood flow to the brain while enhancing the brain's use of oxygen. This can help in conditions such as vertigo, depression, hypertension, and mood changes, all which are often related to insufficient blood flow to the brain.

Warning - Very rarely causes stomach cramps, which will disappear when usage is halted.

Vinpocetine

Benefits - Since vinpocetine and vincamine are both extracts of the periwinkle, they have similar functions. Aids cerebral functions by increasing blood flow to the brain, augmenting brain molecular energy, and fully utilizing glucose and oxygen.

Vinpocetine is used in Europe to treat many illnesses related to poor cerebral circulation, including poor sight, poor hearing, headaches, and memory problems. Vinpocetine has even been tested to improve memory even on healthy subjects.

Warnings - Vinpocetine is safer than vincamine, and it's side effects are rare. They include high blood pressure, dry mouth, and weakness. Vinpocetine has no toxicity.

Phenytoin

Benefits - Phenytoin is known best for its treatment of epilepsy. Phenytoin has been reported to increase several forms of cognition, in particular concentration. It has been shown to have a normalizing effect - persons who experience a lot of anxiety or fear are calmed down, while passive people become more assertive.

Warnings - Sometimes causes a depletion of vitamin B-12 and a increased need for thyroid hormone.

Propranolol Hydrochloride

Benefits - Propranolol Hydrochloride blocks the receptor site for adrenaline in muscular tissues. When someone is afraid, they release large quantities of adrenaline into the bloodstream, causing increased heart rate, etc. Often, this is an undesired effect, particularly when the fear-inducing situation doesn't call for fighting or fleeing. By taking propranolol, you can think clearly when fear would normally prevent such.

Warnings - Lowers blood pressure. Always take propranolol with food, or it will cause nausea. Never take propranolol before an athletic event or when adrenaline would be useful.

Phenylalanine

Phenylalanine is an amino acid that is converted to tyrosine once inside the body, and stimulate mental capabilities. It is a popular ingredient in smart drinks.

Tyrosine

Another amino acid, tyrosine is converted to dopamine, an aggression enhancer and aphrodisiac, when in the body.

Vitamins

Vitamin B-1

Benefits - Vitamin B-1 is an anti-oxidant, protecting the nerve cells from harmful oxidizing agents.

Dosage - 50-1000 mg/day in 3 doses. All B vitamins are water soluble, so the body cannot store them.

Vitamin B-3

Benefits - Niacin has been shown in tests to increase memory in healthy subjects by 10-40%.

Dosage - 50-500 mg/day in 3 doses. At high levels, vitamin B- 3 can cause a "niacin rush," in which a flushing of the skin and tingling occurs. This rush is not harmful, and will disappear after continued use.

Warnings - People with high blood pressure, diabetes and ulcers should only take niacin under a physician's supervision.

Vitamin B-5

Benefits - B-5 enhances stamina and is a anti-oxidant. B-5 is crucial for the formation of steroid hormones, and is necessary for the conversion of acetylcholine from choline.

Dosage - 250-1000 mg/day in 3 doses.

Warnings - Large doses may cause diarrhea. This symptom will disappear after continued use.

Vitamin B-6

Benefits - Crucial for the formation of many neurotransmitters; serontin, dopamine, and norepinephrine in particular.

Dosage - 50-200 mg/day in 3 doses.

Warnings - People using Dopa-L to treat Parkinson's disease should not take B-6. Dosages greater than 200 mg have been shown to cause peripheral neuropathy.

Vitamin B-12

Benefits - B-12 activates the synthesis of RNA in nerve cells, treats depression, fatigue, and headaches.

Dosage - 1 mg/day

Warnings - excessive intake of B-12 may cause nosebleeds or dry mouth.

Vitamin E

Benefits - Vitamin E is a fat-soluble (so the body is able to store) anti-oxidant, which helps delay aging.

Dosage - 100-1000 mg/day.

Warnings - Vitamin E has no known toxicity.

Vitamin C

Benefits - Vitamin C is the chief antioxidant in the body. It is necessary for creating neurotransmiiters and nerve cell formation.

Dosage - 2000-5000 mg/day in 3 doses.

Warnings - Too much Vitamin C can produce diarrhea.