VÍRUS:
SERÃO ESTES TÃO PERIGOSOS PARA OS COMPUTADORES?
E PARA OS SISTEMAS DE ARMAS E DE DEFESA, SERÁ QUE ELES PODEM AFETÁ-LOS?

José Angelo Maciel Monteiro

O artigo aborda, em linguagem acessível para leigos, um assunto de indiscutível importância e atualidade, que já merece ser incluído como de interesse da Segurança Nacional.

Trata-se da interferência nos sistemas computacionais, que tanto pode favorecer uma convulsão social, como a paralisação de uma Força Armada.

INTRODUÇÃO

Uma grande quantidade de informação tem sido disseminada por todo o Brasil, enfocando uma epidemia de vírus que ataca sistematicamente os computadores de uma maneira geral.

Tanto os veículos especializados como aqueles que tratam de temas diversos têm-na citado constantemente em seus artigos, o que mostra uma certa preocupação com o assunto.

O assunto é tão sério que, na Alemanha, existe uma firma que está vendendo um "Sistema

para Construção de Vírus", com o objetivo de gerá-los para os computadores da marca AMIGA, utilizando até 'menu' de seleção.

Embora o assunto possa parecer um problema apenas para os ditos informáticos, ele é muito mais profundo e preocupante, podendo afetar tanto um simples micro usado para deleite de nossos filhos, como o micro da seção onde trabalhamos, ou o sistema bancário onde temos nossas contas. E pasmem, isso já está ocorrendo em bancos de grande reputação aqui no Brasil.

Quando se fala em algo que pode afetar o banco onde temos nossa conta, o assunto deixa de ser dos informáticos para estar ao nível de interesse de toda a sociedade.

Saber o que é o vírus de computador, o que faz, a que nível ele pode nos afetar, é a proposição deste artigo, que enfoca, ao final, a sua participação na danificação ou destruição dos sistemas militares e de segurança de uma nação.

DIMENSÃO DO PROBLEMA

O ataque de vírus nos sistemas de computadores no Brasil, atualmente, é mais comentado no mundo dos microcomputadores, embora eles estejam atuando, também, em grande escala, em computadores de grande porte.

A razão de não aparecer muita informação sobre vírus, abordando computadores de médio e grande porte, é que um menor número de pessoas tem acesso a esse tipo de equipamento e, portanto, a difusão se torna menor. Já no caso dos microcomputadores a situação é inversa.

Existem hoje cerca de 20 milhões de microcomputadores da linha IBM vendidos. Inegavelmente isso favorece o ego dos mal intencionados, pela facilidade de difusão dos vírus.

Similarmente ao vírus biológico, os vírus que atuam nos computadores infestam-nos, danificando o conteúdo dos programas carregados e propagando-se para outros programas presentes nos dispositivos de armazenamento das máquinas.

Equivale dizer que um computador infectado por um vírus, ativo pode infectar qualquer disquete que seja introduzido nele, se não forem tomados determinados cuidados.

Os vírus existem há muito tempo e têm recebido diferentes nomes. O fato é que eles são feitos para interromper o funcionamento do sistema.

As interrupções dos programas não são sempre feitas com propósitos maliciosos. Elas são normalmente projetadas para prevenir sistemas contra usuários inexperientes. Por exemplo,

quando é determinado ao computador para apagar todos os arquivos de um determinado disco, o sistema pára antes da execução, solicitando uma confirmação da ordem.

Outro exemplo é o sistema de controle do uso da CPU (unidade central de processamento) das máquinas de grande porte, que controla o tempo usado em processamento por cada usuário, bloqueando aqueles que ultrapassem seus limites definidos pelo Setor de Operações. Um programa como este pode facilmente ser alterado tornando-se um vírus.

Infelizmente, muitos programadores experientes têm se divertido muito fazendo essas alterações em programas, e gerando, desse modo, diferentes tipos de vírus.

ORIGENS DOS VÍRUS

Alguns acreditam que a raiz do problema das viroses está nos jovens inteligentes e possuidores de uma boa capacitação na área de informática, aliados a uma alta dose de malícia, com habilidade suficiente para imprimir uma mensagem humorística, destruir as informações contidas em uma tela, ou fazer o computador limpar todas as informações do seu disco magnético. Os jovens carregam uma alta dose de culpa.

Alguns vírus são introduzidos, nos computadores através de cópias ilegais, as chamadas 'cópias piratas'.

Um conhecimento profundo da terminologia dos computadores e protocolos de comunicação de dados é necessário, tanto para montar os vírus como para detectá-los.

Na verdade, podemos considerar que os 'micreiros' (viciados em atividades com os microcomputadores), deslumbrados pela criação de um programa que funciona praticamente independente de um comando específico externo, passaram em uma primeira fase a criar os malfadados vírus, sem outro fim que não fosse apenas uma brincadeira.

TIPO DE AÇÃO DO VÍRUS

Os nomes dados aos vírus no passado foram *bomba lógica, bomba de tempo, worm (write once read many)* e *hacking*. Provavelmente, todas foram feitas para interromper sistemas.

Bomba lógica. É uma ação que foi utilizada por programadores de grandes sistemas até pouco tempo e que ainda é possível ser empregada.

Trata-se de um pedaço de código embutido num programa criado. Esse pedaço de código só entra em atuação se certa instrução ou item for verdadeiro. Daí o nome de bomba lógica.

Suponhamos um programador descontente e que trabalhe no projeto da folha de pagamento de sua firma. Preocupado com sua futura demissão, esse elemento poderia escrever um pedaço de código embutido no programa principal, de modo que, se as suas informações pessoais não fossem encontradas na folha de pagamento, o sistema automaticamente desviaria para uma outra parte do próprio sistema ou para outra área do disco. Dentro da mesma idéia, o código poderia determinar ao programa que o reincluísse na folha de pagamento, regravando, na fita de computador que vai para o banco, suas informações cadastrais e o correspondente vencimento.

O desvio no programa poderia levar a uma outra parte do próprio programa, ou a outro programa que, quando acionado, começasse a apagar registros de informação do banco e dados do sistema.

É muito difícil determinar a existência de uma bomba lógica. Por isso, torna-se importante que todo trabalho de programação seja revisado e testado por outro programador ou supervisor. Essa atitude não previne a ocorrência de armadilhas de programação, mas já dificulta a geração das mesmas.

Bomba de tempo. Similarmente à bomba lógica, existe a bomba de tempo, detonada a partir de certa contagem de tempo ou de certa data. Quando o ponto de referência for atingido, o programa inicia suas atividades nefastas criadas pelo maquiavélico programador.

Write Once, Read Many (WORM). Esse tipo é copiado para a memória principal do computador, toda vez que este é ligado. Durante as interrupções normais de processamento, onde o processador, por exemplo, lê as informações do teclado, do vídeo, ou grava um arquivo, o WORM, paralelamente, cria danos inicialmente imperceptíveis.

Por exemplo, quando você cria um arquivo num processador de palavras e o armazena no disco, você recebe as informações de que o arquivo foi armazenado (salvo). Entretanto, durante o procedimento para o armazenamento, o vírus permite que somente parte do arquivo seja salvo, ou mesmo que partes desse arquivo sejam substituídas por espaços brancos ou outros caracteres. Desta forma, na próxima fase que você tentar carregar esse arquivo, ele estará incompleto ou sem sentido.

Algumas casas especializadas em comercialização de software (Software Houses) freqüentemente se utilizam do WORM para proteger seus softwares contra pirataria. Dessa maneira, o WORM introduzido no software vendido não permite

a cópia parcial ou integral do sistema vendido. Quando é tentada a cópia, o sistema dá a informação de "cópia ilegal".

Sistemas que operam em rede, através de modems, multiplex etc., são mais preocupantes, por serem vulneráveis ao acesso não autorizado.

Algumas pessoas têm por *hobby* xeretar os sistemas alheios. Após o acesso à rede de dados, uns costumam apenas dar uma olhada no tipo de trabalho que está sendo desenvolvido; outros só se dão por satisfeitos após alterar ou danificar o conteúdo daquilo que foi violado.

Essas pessoas são conhecidas, no exterior, como *hackers* e, para se ter uma idéia do grau de organização em que se encontram, pode-se citar que mais de duzentos deles se reuniram, em agosto deste ano, em Amsterdam (Holanda). Vieram dos Estados Unidos e de toda a Europa para um congresso chamado Festa Galáctica. Nele debateram as mais recentes técnicas de acesso às redes e bancos de dados privados.

Embora esse grupo esteja trabalhando em algo que nos repudia à primeira vista, na realidade eles prestam um grande favor, ao evidenciar as falhas de segurança dos sistemas considerados seguros.

A INFESTAÇÃO DO VÍRUS

A infestação pode começar, por exemplo, quando uma pessoa copia um arquivo (um programa) do disquete de um amigo. Supondo-se que este arquivo estivesse previamente contaminado, o 'pirata' passou a ter, assim, vírus latente em seu disquete.

A partir daí, quando o 'pirata' executar o programa para ver o que o mesmo faz, o vírus presente no programa copiado transfere-se para a memória principal e, de lá, reproduz seu código em outros programas, infestando mais e mais o resto do conteúdo do disquete ou do disco rígido do computador.

A ATIVAÇÃO DO VÍRUS

O vírus instalado necessita de algo para ser ativado. Algo para colocá-lo em atividade e gerar o dano ou a brincadeira desejada por seu criador. Aí é que entra a genialidade dos 'micreiros'.

A instalação e o espalhamento é sempre muito simples e eficiente. Requer, naturalmente, ações normais do usuário como executar um programa que esteja armazenado em um disquete (programa pirateado ou de um terceiro), executar alguns comandos do sistema operacional, ou, então, iniciar o sistema utili-

zando um disquete contaminado.

A iniciação utilizando disquete é freqüentemente utilizada em joguinhos de computador, que obrigam o carregamento do sistema na máquina através do próprio disquete.

Os vírus, que se ativam pelo simples uso dos comandos do sistema operacional, instalam-se na memória principal e permitem sua posterior migração para outros programas durante o uso continuado da máquina.

Existem ainda outras formas de disparo da *peste* que merecem ser consideradas. Uma chave numérica pode ser usada para a eclosão do surto de vírus no computador. Utilizando-se um contador, que contabilize a base de tempo gerada pelo relógio interno do computador, um número é atingido. Esse número permite um desvio do programa para uma rotina externa, a *rotina virótica.*

A rotina virótica pode ser ativada, também, em uma determinada data-chave estabelecida durante a confecção do programa. Nesse caso, o sistema fica vigilante para ser acionado, apenas, quando essa determinada data-chave for atingida.

Fica evidente que aquele que gerou esse tipo de vírus pode ficar vigilante, de modo a alterar os parâmetros de disparo para uma época oportuna.

É importante ter em mente que o que caracteriza um vírus é sua capacidade de espalhamento de máquina para máquina. É interessante abordar esse ato, tendo em vista que existem outros tipos de programas que produzem danos e destruição aos discos, embora não tenham capacidade migratória.

Os programas dessa família são chamados *Cavalos de Tróia* e simulam executar uma tarefa, enquanto, na verdade, realizam outra bem diferente. Normalmente têm nomes que sugerem operações de apoio ou manutenção de arquivos, realizando, entretanto, tarefas destrutivas.

Suponhamos, para exemplificar, um software que trabalhe em simulação onde são necessários cenários. Esse software necessita um programa que carregue no computador os novos cenários. O nome do programa que faz o carregamento do cenário poderia ser CENÁRIO. Um "Cavalo de Tróia" com nome de CENÁRIO II poderia ser criado para apagar os programas de cenários, quando fosse executado. O operador, estimulado pelo nome CENÁRIO II o executaria, obtendo tristes conseqüências.

JERUSALÉM E PING-PONG

No Brasil, dois tipos de vírus, dentre os já identificados no mundo, têm infectado os mi-

crocomputadores: o vírus da Universidade Hebraica, conhecido como Jerusalém (ou Israei ou Sexta-feira 13) e o Ping-Pong.

O vírus Jerusalém atua na linha dos microcomputadores IBM–PC, e se copia automaticamente para os arquivos executáveis e do sistema operacional.

Arquivos executáveis são programas que executam uma tarefa predeterminada. Seus nomes são seguidos de um ponto e terminações BAT, EXE e COM.

O vírus Jerusalém também contamina os arquivos de extensão SYS, pertencentes ao sistema operacional.

Os sintomas desse vírus são basicamente os descritos a seguir.

Em todo dia 13 de qualquer mês, o sistema torna-se lento e atua extremamente estranho, aparecendo 'lixo' (caracteres estranhos) na tela.

Além disso, em qualquer sexta-feira 13, exceto as do ano de 1987, o vírus provoca uma 'autodestruição' que causa, a cada comando executado, o apagamento dos arquivos executáveis. A mensagem *Bad Command or file name* aparece a todo comando executado, causando espanto no operador.

Um usuário experiente poderá notar que o vírus Jerusalém aumenta o tamanho dos arquivos EXE grosseiramente na ordem de 1800 bytes, após cada execução, e que os arquivos do tipo COM crescem apenas 1800 bytes, independentemente do número de execuções.

Com o uso de um programa auxiliar de manutenção, pode-se observar, na Figura 01, informações de parte de um arquivo executável (MARK. COM).

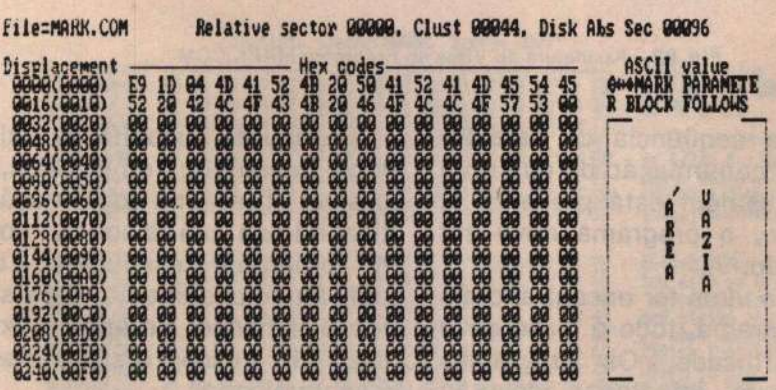

Fig. 01 – Trecho do Programa MARK.COM sem Vírus Jerusálem

As numerações abaixo das palavras HEX CODES correspondem, da esquerda para a direita e de cima para baixo, às sucessivas instruções que compõem este programa e que são interpretadas pelo computador como tarefas a executar seqüencialmente.

A coluna da direita apresenta a parte correspondente dos HEX CODES do programa onde podemos visualizar algumas letras.

Na Figura 02, que corresponde ao mesmo trecho da Figura 01, observamos que a área anteriormente vazia está agora completamente ocupada por caracteres estranhos, surgindo, logo no início da área, a seqüência de caracteres "SUMsDos", que podemos considerar a assinatura do vírus Jerusalém.

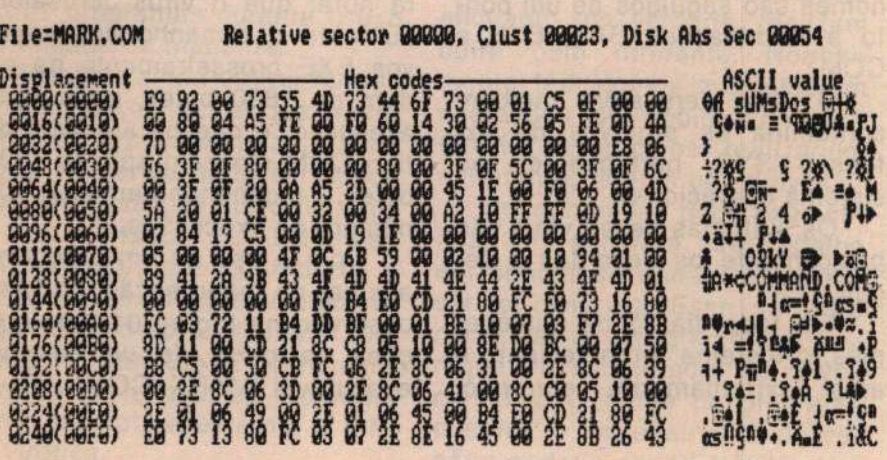

Fig. 02 – Assinatura do Vírus no Programa MARK.COM

Esta seqüência de caracteres é a confirmação de que o vírus Jerusalém está presente e, portanto, o programa deve ser destruído.

Se o vírus for encontrado em um programa, todo o disco deve ser verificado. Os programas porventura infectados deverão ser apagados e substituídos por novas cópias.

Se houver suspeita da existência desse vírus no sistema, é possível obter uma confirmação, utilizando-se um disquete com um programa executável, do qual, antecipadamente, seja sabido o tamanho. Se após a execução ele crescer, o sistema está contaminado.

O vírus Ping-Pong se aloja na

área de inicialização do disco (setor de BOOT).

O setor de *boot* possui informações que permitem ao computador copiar, do disquete para a memória eletrônica (RAM), o Sistema Operacional.

Na Figura 03 é possível, do mesmo modo que na Figura 02, observar as instruções do setor de BOOT do disco. À direita é encontrado, a partir da terceira linha, um espaço em branco, e, nas últimas linhas, podemos verificar algumas informações legíveis.

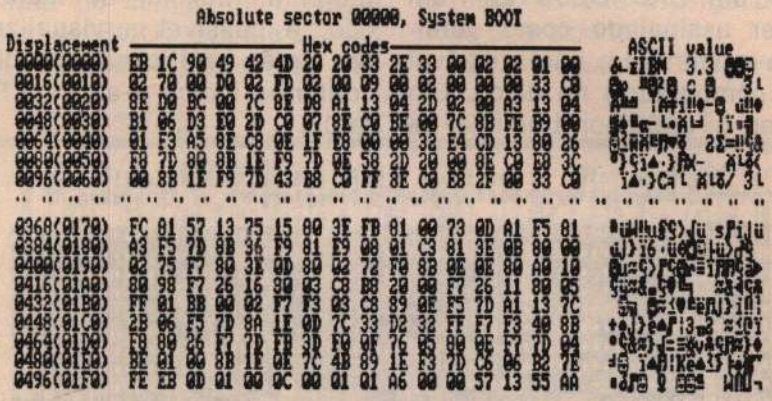

Fig. 03 – Área de BOOT Sadia

A seguir, na Figura 04, correspondendo à mesma porção da figura anterior, é observado o desaparecimento tanto do espaço em branco como das mensagens da parte inferior. Praticamente desapareceram os textos legíveis.

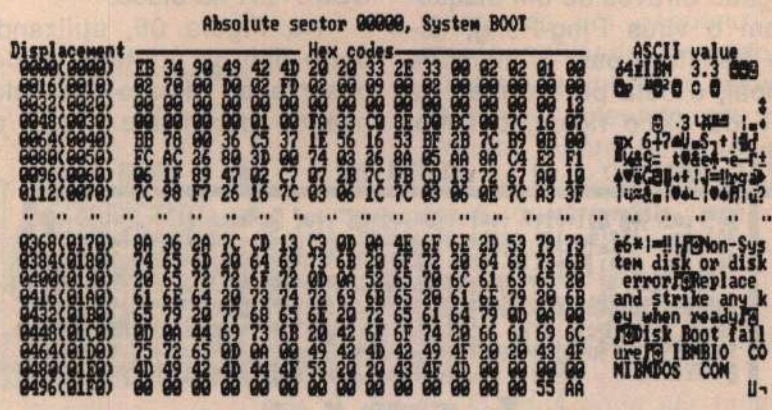

Fig. 04 – Setor de BOOT Infectado pelo Vírus Ping-Pong

O Ping-Pong, como foi dito, aloja-se no setor de BOOT. Como este setor não é suficientemente grande para alojar o procedimento de carga (BOOT) adicionado do código do vírus, o próprio vírus se encarrega de criar uma área pseudo danificada – um BAD CLUSTER (um cluster assinalado como defeituoso e, portanto, não utilizável pelo computador) no disco. Um cluster é a menor unidade de armazenamento de dados em disquete/winchester – um arquivo por menor que seja ocupa 1 cluster. Para esta área o vírus transfere parte dele mesmo e parte do procedimento de carga.

Novamente, através de um programa auxiliar de manutenção, é possível a visualização da área danificada do disco, conforme indica a seta na Figura 05.

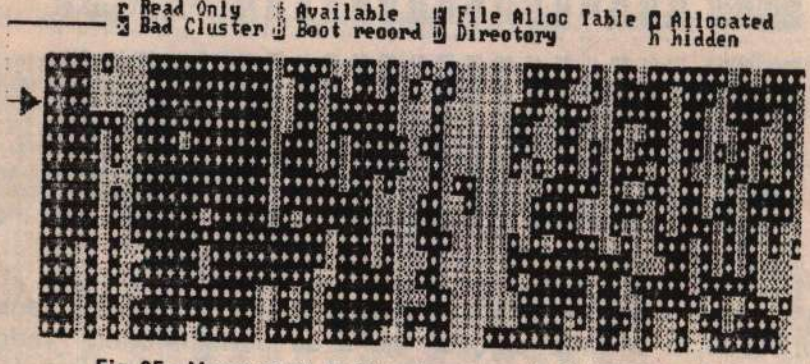

Fig. 05 – Mapeamento do Disco Apresentando CLUSTER RUIM

Toda vez que o sistema é carregado através de um disquete com o vírus Ping-Pong, este se transfere para a memória principal, e dela para a área de BOOT do disco rígido, criando, conseqüentemente, um BAD CLUSTER no disco.

Na Figura 06, utilizando-se outro tipo de utilitário, pode ser observado, dentro do cluster pseudo danificado (79.1) parte

Fig. 06 – CLUSTER Infectado pelo Vírus Ping-Pong

do código deste vírus. Na última linha observa-se uma seqüência de quatro caracteres iguais, que poderia ser tomada como referência para a presença do vírus.

Na Figura 07, é apresentada a continuação do cluster pseudo danificado (79.1). É observado o restante do código de carregamento do BOOT (cluster 79.2). Nele podemos observar as mesmas palavras legíveis discutidas anteriormente, na Figura 03.

Assim, na área pseudo danificada é encontrada a parte do código de carregamento que foi transferida. É possível concluir que o vírus é carregado e, em seguida, é feita a carga do sistema operacional.

O sintoma do Ping-Pong é

Fig. 07 – Final de Registro de BOOT Deslocado para um CLISTER RUIM

Fig. 08

apresentado através do surgimento de um pequeno ponto, com aproximadamente dois milímetros de diâmetro, movendo-se e ricocheteando nas bordas da tela. Aparentemente inofensivo, o vírus vai ocupando as áreas de memória, até causar um colapso no sistema que deverá ser novamente carregado.

A ação do Ping-Pong é similar à apresentada na Figura 08.

O vírus pode ser facilmente eliminado, recarregando-se o

sistema a partir da unidade de disco flexível, com um disco sadio e protegido. Para sanar o problema, através do utilitário SYS COM, transfere-se o sistema sadio para os discos infectados.

Os clusters eventualmente apresentados como ruins (BAD CLUSTER) devem ser liberados para não se ter diminuída a capacidade do disco.

COMO SE PROTEGER DOS VÍRUS

Cada vírus atua de uma forma específica. Portanto, é necessário, após a sua detecção e estudo do modo de ação, uma receita específica para proteger os computadores. Como foi dito, hoje existem catalogados diversos vírus no mundo. Isso leva a crer que necessitaríamos criar uma infinidade de vacinas antivírus.

As rotinas de pesquisas dos vírus demandam um gasto de tempo de processamento, diminuindo, conseqüentemente, a performance do equipamento.

Assim, seria criado um problema semelhante ao surgido com a área de comunicações nos computadores de grande porte. Hoje, esses sistemas possuem um computador principal (HOST), para processamento de dados, e um outro computador (FEP), destinado apenas às tarefas de comunicações.

Seria necessário, portanto, um computador específico para as atividades antivírus.

Não é esta a saída. Antes de tudo é necessária uma maior preocupação com a segurança da informação. É preciso uma conscientização de certos procedimentos profiláticos que gerem uma barreira contra o vírus e barrem os caminhos por onde ele costuma penetrar.

SUGESTÕES DE PROTEÇÃO PREVENTIVA

Se o Centro de Processamento de Dados (CPD) só utiliza softwares comprados de fontes legítimas e não permite a inicialização do sistema através de discos externos, o risco diminui. Mas se, por outro lado, o CPD é daqueles que copiaram o software do Paulo, que copiou do Antonio, que copiou do João, que tinha um software contaminado, então ele está provavelmente vulnerável.

É importante não permitir a utilização dos computadores do CPD para joguinhos. Estes, pelo seu carregamento, por comando ou por inicialização do sistema, favorecem a contaminação.

É necessário criar normas gerais de utilização dos softwares, tais como: obrigar a utilização apenas de cópias *(Back-up)* dos originais de softwares comprados ou contratados, bem como dos sistemas desenvolvidos.

Assim, estar-se-ia preservando os softwares para recarga quando as dúvidas surgirem.

A utilização dos discos originais e suas cópias devem ser feitas sempre com o selo de proteção contra gravação, para não permitir que um vírus instalado na memória principal possa infectar o disquete em uso.

Softwares de domínio público, ou seja, aqueles que acompanham determinadas revistas especializadas, fornecidos como brindes através de disquetes, nunca devem ser carregados diretamente nos discos rígidos. É necessário uma quarentena antes da instalação. Deve-se testar o software em computadores que usem somente drives.

Para se ter uma idéia, de acordo com informações publicadas no exterior, um delinqüente modificou um programa antivírus, de domínio público, transformando-o exatamente no contrário. O programa passou, dessa maneira, a contaminar os arquivos daqueles que buscavam uma solução para suas possíveis viroses.

Em ambientes comerciais, onde os programadores trabalham em regime integral, é fácil para um empregado inseguro ou insatisfeito escrever, no meio de um programa, uma rotina que execute a tarefa de apagar registros do sistema após uma determinada data, ou outro evento esperado. Essa rotina de apagar o registro poderá estar codificada no programa ou fora dele.

O sistema passará, naquela parte do programa, a testar uma data ou um evento programado, toda vez que o programa for executado. Quando a data ou evento chegar, o sistema automaticamente executará sua função de apagamento.

Este programador maquiavélico poderá ir modificando a data ou evento de disparo da sabotagem, de forma a não permitir o disparo em épocas não oportunas. Por exemplo, enquanto ele estivesse empregado, a data ou evento não dispararia.

Um sistema de gerenciamento que permitisse, por exemplo, outro programador verificar o código do programa em questão, antes que ele entre em execução, poderia, perfeitamente, desarmar esse tipo de "bomba de tempo".

Além disso, é necessário que os programadores trabalhem em grupos criados aleatoriamente, para que uns sejam os fiscais dos outros.

É de capital importância criar, no CPD, a função de supervisor, atribuindo a ele a responsabilidade de verificar os procedimentos abordados e fiscalizar se a utilização dos novos softwares em uso foi introduzida com a autorização da gerência do CPD.

É importante considerar que os danos causados a semelhantes sistemas devem ser encarados como crime perante a lei, pois são tão danosos como entrar na sala do Centro de Processamento de Dados, munido de uma marreta, e destruir alguns equipamentos. Na verdade, as duas formas param os sistemas com prejuízos.

SISTEMAS QUE TRABALHAM EM REDE DE DADOS

Recentemente, a virose tem afetado computadores nos quais os usuários acessam redes de domínio público. As redes permitem, aos que as integram, partilhar seus softwares livremente (software feito pelo próprio usuário ou não). A grande conseqüência disso é que programas são intercambiados e, durante essa troca, o vírus pode migrar de máquina para máquina. Pouco se pode fazer nesse caso.

Nos locais onde os funcionários trabalham com redes, o acesso à rede deve ser restrito. Deve-se evitar a entrada nas redes privadas externas e a troca de software com outras máquinas. Um supervisor deveria checar constantemente o conteúdo dos discos, para se assegurar que os softwares existentes são os permitidos.

O acesso ao conteúdo dos discos de outros computadores deve ser bloqueado, não permitindo assim a pirataria.

As redes de dados são muito atingidas pelos já mencionados Hackers. É o caso de representantes da pirataria alemã, que foram expulsos dos Estados Unidos, no começo do ano, devido à acusação de violar sistemas militares americanos através do serviço secreto soviético.

UM CASO REAL

Programas com vírus têm sido introduzidos nos sistemas, usualmente através de transmissão de dados na rede de teleprocessamento.

Em dezembro de 1987, foi introduzida uma "bomba de tempo" nas redes de dados de um país da Europa. Foi a vez do vírus conhecido como a árvore IBM CHRISTMAS. Este vírus gerava uma saudação de natal e desenhava um pinheiro na tela.

Toda vez que um novo usuário acessava a rede de computadores ele era saudado com uma mensagem e com o desenho. Simultaneamente, o vírus era recopiado na rede, consumindo tempo, memória, entravando as linhas e reduzindo, drasticamente, o tempo de resposta do sistema de teleprocessamento.

PROTEÇÃO DE REDES

Para evitar casos que envolvam rede, os gerentes de centros de processamentos de dados (CPD) devem revisar com cuidado os seus critérios de acesso.

Além dos sistemas de senhas para acessar as redes, há necessidade de se implementar softwares que monitorem e contabilizem o número de vezes que um determinado terminal tenta acessar o CPD. Se não houver sucesso (por exemplo, após três tentativas), o acesso do terminal deve ser cortado, bem como alertado o operador do equipamento para providências.

Além disso, o sistema deve registrar o número de ocorrências desses eventos e outras informações, gerando um arquivo que facilite a identificação e captura do intruso.

É necessário colocar senhas nos sistemas existentes, com o mesmo tipo de controle de contabilidade descrito no parágrafo anterior.

É necessário, também, organizar os arquivos de modo a proibir a cópia e a leitura por pessoas não autorizadas, registrando, da mesma forma, as tentativas de leitura e cópia para análise e devidas providências pelo setor de operações.

Ações desse tipo diminuem a possibilidade da tentativa de intrusos em abrir as chaves dos sistemas e, a partir daí, roubar ou danificar informações.

É muito pouco o que se pode fazer para evitar que uma máquina nunca seja violada via rede de dados. Entretanto, fornecer uma orientação ao pessoal, através de uma doutrina de uso de Hardware e Software, bem como do acesso às redes de dados, ajudarão muito na prevenção contra os vírus.

E NA ÁREA MILITAR?

Na área militar, a utilização de vírus tem surgido através da drenagem de bancos de dados dos países de interesse, bem como no espalhamento de vírus pelas máquinas desses países.

Conforme noticiado pela revista *Time* de março de 1989 no início de 1981 a Agência Nacional de Segurança descobriu que alguém havia conseguido obter uma considerável quantidade de informações sigilosas, através do acesso a um cabo 'protegido' que ligava uma determinada instalação de informações à sua rede. A espionagem foi atribuída a elementos do bloco oriental.

Em ocasiões anteriores, outras espionagens sofisticadas já haviam sido detectadas. Serviços de Informações de ambos os lados se revezaram em ações dessa natureza.

Na terceira semana de março, os EUA expulsaram um adido militar soviético, por suspeitarem que ele tentara roubar detalhes de programas de segurança de computadores. Da mesma forma, outros três alemães orientais, violadores de computador, foram presos, suspeitos de espionar para a União Soviética.

Esses alemães, possivelmente acessaram trinta computadores não sigilosos da defesa dos EUA e tentaram, ainda, acessar outros 420. Pareciam estar mapeando o sistema de defesa americano, à procura dos acessos não permitidos, levantando, dessa maneira, os sistemas sigilosos.

Esses fatos mostram a preocupação das agências de informações em encontrar maneiras de penetrar nos sistemas de se gurança uma das outras.

Segundo o informe, as agências de informações americanas têm obtido sucesso considerável em penetrar nos sistemas computacionais militares, sigilosos, da União Soviética e, também, de outros países. A regra é simples, pois em qualquer país onde as comunicações são delicadas, é possível interceptá-las e, evidentemente, ler informações dos computadores. Enfim, entrar naquele universo de informações.

Atualmente, as grandes potências procuram provocar desordens nos computadores de outros países, infectando-os com alguns tipos de vírus e programas destrutivos.

A crescente dependência dos sistemas militares em redes de computadores interligados, de modo a permitir a supervisão, o comando e o controle no campo de batalha, aumenta a possibilidade de sabotagens por agentes possivelmente infiltrados.

É fácil supor um sistema de coordenação e controle que, em tempo de paz, foi infectado por um vírus, que permanece latente aguardando uma oportunidade de eclodir.

O vírus poderia, por exemplo, estar incubado no sistema de dados do controle das armas, do sistema de Artilharia Antiaérea de um determinado país, aguardando o início das hostilidades. No recrudescer das ações, o agente infiltrado, aquele que escreveu o programa e o inseriu no software, envia ao sistema uma palavra-chave que, ao ser recebida, passa a danificar os dados dos computadores ou, por exemplo, passa a trocar os dados dos cálculos dos radares passando a apresentar informações incorretas e a fornecer apoio a decisões totalmente erradas. Um maravilhoso campo para se investir.

Tal vírus, agindo desta forma, poderia mandar entregar os suprimentos em locais diferen-

tes ou mesmo, despachá-los de modo errôneo aos destinos. Por exemplo, capas de chuva ao invés de abrigos de frio.

É possível se discordar quanto à maneira como seria feita essa sabotagem, mas inegavelmente ela é possível, e já vem ocorrendo. O potencial ofensivo dele é tão grande nos exércitos modernos que poderia paralizar suas forças, à semelhança das grandes armas nucleares.

UM CASO FICTÍCIO

Necessitando reaparelhar seus exércitos, o país Azul comprou recentemente da superpotência Z, equipamentos de Guerra Eletrônica (GE), artilharia antiaérea (AAAé) e equipamentos de identificação amigo-inimigo (IFF) para seus equipamentos de tiro, todos baseados na tecnologia de ponta e apoiados em informática.

A superpotência Z possui laços étnicos e históricos profundos com o pais Vermelho.

No momento, está ocorrendo uma crise internacional em torno de um território litigioso entre os países Azul e Vermelho.

As negociações diplomáticas, para resolver as conflitantes reclamações de soberania, não deram certo e foram rompidas.

Existe uma situação de tensão e um efetivo considerado de tropas regulares se deslocou para a região em ambos os lados.

As atividades de Medidas Eletrônicas de Apoio (MEA), foram executadas por ambos os lados em tempo de paz.

O país Azul, mais experiente, detalhou, através de seus sistemas de GE, a estratégia das autoridades políticas, militares e de segurança interna, e espera tirar bom proveito do seu trabalho.

O conflito é iminente e, devido a isso, as tropas de Guerra Eletrônica e Artilharia Antiaérea do país Azul já estão desdobradas.

O país Vermelho, recorrendo a seus laços históricos, recebeu inestimável auxílio da superpotência Z; as palavras-chave para detonar as "bombas lógicas" que ela imbutiu nos softwares, tanto de comunicação de dados como dos próprios sistemas de GE e AAAé, antes de vendê-los ao país Azul.

Conhecedores do protocolo de comunicações utilizado no material bélico vendido, a superpotência Z repassou-os ao país Vermelho, junto com as palavras-chave.

Essas palavras serão transmitidas por um transmissor idêntico ao utilizado por aqueles equipamentos e enviadas pelo mesmo protocolo em uso. Após a detonação da "bomba lógica", os sistemas de GE perderão

seus arquivos de dados e os de AAAé ficarão tão lentos que não conseguirão apoiar nenhuma decisão quanto aos alvos.

Possivelmente, ocorrências tão sutis demandarão grande tempo em suas pesquisas e jamais permitirão comprometer Z.

Impossível ??!!

CONCLUSÕES

Quando, na época dos romanos, a catapulta inovou as armas de arremesso, nenhum romano ousou pensar que os chineses inventariam a pólvora, que, usada em uma nova arma, a ser criada, tiraria as magníficas catapultas de circulação.

Quando as blindagens apareceram nos campos de batalha, o impacto também foi muito forte, e ninguém pensou que surgiriam mísseis anticarro para contrabalançar o campo de batalha. Hoje, as blindagens de sacrifício já se contrapõem a alguns destes artefatos, dando continuidade ao desenvolvimento.

Inventaram o rádio para se levar informações com maior rapidez e logo surgiram o interferidor, e as intrusões, com mensagens falsas, para alarmar e desacreditar o sistema. No entanto, ele aí está, mais do que nunca, com seus processos de salto de freqüências, *burts* e espalhamento no espectro.

Na realidade, não se pode fugir ao momento tecnológico da informática, pois hoje, mais do que nunca, e em qualquer área, vence aquele que detém a informação. Vence aquele que as processa de maneira mais rápida e eficiente.

Apesar de todas as informações a respeito de vírus, na realidade, o problema não é tão grave assim. Muitas reclamações atribuídas a ele não passam de conhecimento insuficiente do equipamento, do software utilizado e da falta de experiência do operador.

Deve ser levado em conta, também, que o pânico gerado pela epidemia e sua divulgação traz muitas vantagens para alguns grupos (os vendedores de equipamentos e softwares).

De um ponto de vista bem otimista, é até bom o surgimento dos vírus, porque está mostrando a fragilidade de nossos sistemas.

Através da tão falada epidemia, passaremos a ter uma maior consciência do tratamento de nossas informações e dos processos que permitem a compra de determinados softwares.

Quem nos garante que dentro de um pacote bélico específico, ou mesmo administrativo, o vendedor já não deixou embutido uma bomba de tempo? Suponhamos que um país possuidor de um sistema desse tipo entre em conflito com um país

aliado da firma vendedora do produto. Será que o aliado poderia ativar uma bomba de tempo, ou de qualquer outro tipo, para neutralizar os sistemas militares existentes?

O que se tem a fazer, no momento, é criar uma consciência voltada para a segurança dos dados a todos os níveis. E assegurar que esses computadores que participam de redes trabalhem em ligações com outros sistemas adequadamente protegidos por equipamentos de codificação, bem como funcionem com proteções contra tentativas de acesso, quebrando a rede e possibilitando pistas para o descobrimento do violador.

Há que se implementar os setores de suporte técnico dos CPDs, colocando-se grupos que montem sistemas supervisores, para que se analise e intercepte os intrusores antes de seu sucesso.

Há que se criar supervisores junto aos elementos que estão desenvolvendo novos sistemas e junto àqueles que estão realizando manutenção nos sistemas existentes.

Na realidade, apènas o ambiente mudou. Os problemas de segurança permanecerão como sempre. O que se tem a fazer é investir em cérebros que estudem amiúde os computadores, os softwares contratados e os de teleprocessamento. Não mais é possível permitir que os novos projetos em desenvolvimento tenham a parte de programação feita por um único homem.

Os problemas de controle da informação são os mesmos que surgiram desde o tempo do início da civilização. Alguém detém a informação que alguém quer ter. O que mudou foi apenas o processo como obter ou deturpar essas informações.

O Major Com JOSÉ ANGELO MACIEL MONTEIRO, é Aspirante da Turma de 1972. Possui os seguintes cursos: EsAO, em 1982; Análise de Sistemas, IME, 1984; Organização e Métodos, SEPLAN, 1985; Communications Delivery Installation Workshop, UNIVAC, 1986; Electronic Warfare, England, 1986; Electronic Warface, Germany. 1988; Avaliação de Guerra Eletrônica, IPD, 1988 e Guerra Eletrônica, CIGE, 1989.

Atualmente chefia a Seção de Informática do Centro de Instrução de Guerra Eletrônica

---