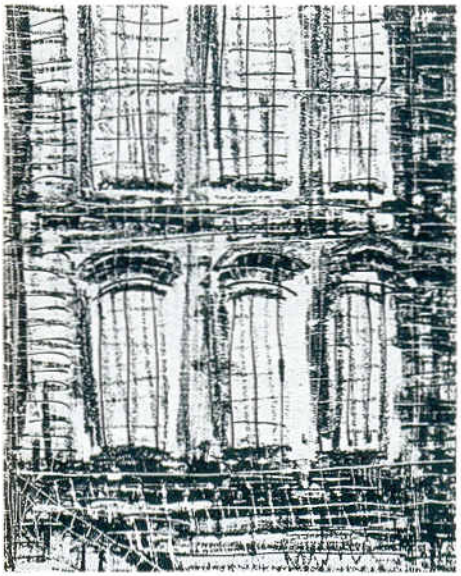

SEGURANÇA UM BREVE TUTORIAL

George Leal Jamil

Os ataques a instalações de informática têm-se tornado cinematográficos. A mera ameaça, ou boatos a respeito, já merecem destaque em órgãos da imprensa e da própria Internet. Denúncias de roubo de acervos, violações de privacidade, abertura ilegal de conteúdos, impedimento de serviços e outros têm sido freqüentes, aumentando a preocupação de usuários e sendo uma contrapartida à evolução dos próprios serviços eletrônicos.

Por exemplo, consideremos os casos envolvendo cartões de crédito. Meio de pagamento inegavelmente rápido, ágil e versátil, esses cartões têm sido alvo constante de abordagens e tentativas por parte dos espiões e malfeitores. Apesar da imagem de roubo de senhas e acessos, já foram encontradas milhares de senhas em poder de um único criminoso, que apenas as mantinha em seu poder como se fosse um "colecionador".

Os provedores de informações sofrem com as tentativas de alteração de suas páginas, envios de e-mails falsos, clonagem de sites, informações truncadas e dispersas, usuários fictícios, etc.

Outros casos envolvem prestadores de serviços na rede, como os provedores de informações e serviços de e-mail. Os provedores de informações sofrem com as tentativas de alteração de suas páginas, envios de e-mails falsos, clonagem de sites,

informações truncadas e dispersas, usuários fictícios, etc. Os novos sites de e-business tornam-se atrativos para roubos e vandalismo eletrônico. Vamos abordar, neste artigo, alguns dos tipos mais habituais de ataques.

Alteração de domínios

Consiste na troca de endereçamento real de determinados domínios da Internet. Ao digitar, por exemplo, www.banco.com, um possível cliente do "banco" é encaminhado para outro site que não o original, porque algum criminoso alterou o endereço final de acesso. Dessa forma, se o site for "clonado", o usuário poderá digitar informações e fornecer dados sigilosos, que estarão de posse dos detentores dessa cópia.

Esse mecanismo já foi utilizado para cópia de sites de acesso a bancos, órgãos públicos e serviços de mídia, levando usuários à confusão e causando transtornos para os reais detentores. Em 1997, ocorreu a distribuição na rede de uma tabela de tradução de domínios (serviço DNS) que continha erros. Apenas esse dano involuntário ocasionou indisponibilidade e grandes problemas no uso da Internet, seu impacto tendo sido sentido por dias (muitos servidores são atualizados automaticamente, sem intervenção humana, e passaram a falhar, então).

O problema com esses arquivos malignos é o fato de, com sua identificação falsa, iludirem os usuários, pois têm nomes divertidos ou relativos a fatos recentes, que enganam aqueles que os recebem.

Idêntico ao fato enunciado pelos contos épicos, esses arquivos – geralmente executáveis – têm um nome, uma hipotética identidade, mas realizam outras atividades. Entre as características, há programas que, enquanto exibem informações ou animações, vão, em paralelo, destruindo os seus arquivos em disco rígido; outros apagam arquivos com algumas extensões e assim por diante.

O problema com esses arquivos malignos é o fato de, com sua identificação falsa, iludirem os usuários, pois têm nomes divertidos ou relativos a fatos recentes, que enganam aqueles que os recebem. A prevenção, nesses casos, fica substancialmente dificultada. Casos como esses foram os recentes "Happy99", "Iloveyou" e variações, em que os nomes e identificações de mensagens e arquivos anexos iludiam os usuários, fazendo-os não só serem infectados, mas participarem

involuntariamente do processo de distribuição dos mesmos, que se replicam de forma automática.

Roubos de senha

Os terminais de vídeo e as estações conectadas em rede habitualmente possuem um pequeno programa, por vezes chamado de "monitor", que permite um nível limitado de programação – para, por exemplo, utilizar recursos gráficos de tela, como vídeos reversos, piscantes, brilhantes, etc. Um recurso eletrônico utilizado para acesso indevido às senhas e códigos de usuários (pode ser, por exemplo, um número de conta bancária ou de cartão de crédito) é desenvolver e instalar ali um programa que simule o processo de login em uma rede.

Uma vez em execução, esse programa irá permitir ao seu proprietário conhecer todas as entradas emitidas pelo usuário, "abrindo" a identificação digitada, capacitando-o a usá-la posteriormente. Já presenciamos o uso de funções de suporte desse programa monitor em terminais de vídeo. Ao serem ativadas, emitiam os códigos hexadecimais dos caracteres digitados em tela. Ao invasor bastava traduzir os códigos, usando uma simples tabela de transcrição, e ter acesso aos dígitos informados, passando a poder "logar-se" como aquele usuário.

Esse tipo de ação deu origem a tipos de vírus e "vermes" que capturam códigos e senhas em redes e em sistemas multiusuários, "quebrando" a segurança dos mesmos, liberando essas informações aos invasores.

Ddos - Denial of Service

Verdadeiro "sucesso" de ataques no início do ano 2000, esses crimes consistiram na replicação de um programa que encaminharia requisições a sites de comércio eletrônico e prestação de serviços ininterruptamente, assim que ativados. Essas cópias ficaram armazenadas em instalações que os atacantes tiveram possibilidade de invadir.

Ao alocar, continuamente, recursos para o atendimento às requisições encaminhadas, o site de serviços acabava por não conseguir atender à demanda, pela simples exaustão de capacidade, pela falta de recursos de memória e banda.

Uma vez "chegada a hora", os requisitores de serviços (como, por exemplo, chamadas de servidores de e-mail) iniciavam um processo sistemático de requisição, chegando, no total, a encaminhar centenas de milhares de solicitações a um mesmo endereço. Ao alocar, continuamente, recursos para o atendimento às

requisições encaminhadas, o site de serviços acabava por não conseguir atender à demanda, pela simples exaustão de capacidade, pela falta de recursos de memória e banda.
As demais requisições – muitas delas verdadeiras – não podiam, portanto, ser atendidas.
Alguns desses sites passaram horas indisponíveis, o que fez a contabilização de centenas de milhares de dólares em perspectivas de negócios não realizados. Ocorre, portanto, o impedimento ao uso dos serviços. Existem algumas variações desse tipo de dano, tendo como alvo instalações de difusão de sinais de áudio e vídeo, servidores de FTP e WWW.

Invasões de Sites (Backdoor)

Funcionam ao instalar num computador conectado a uma rede um programa- cliente que permite a um programa servidor utilizar essa máquina sem restrições. Esses programas foram desenvolvidos originariamente para tele-atendimento, útil função pela qual um profissional de suporte controla a máquina de um usuário, visando a esclarecer uma dúvida ou verificar um problema operacional qualquer.

A exemplo dos vírus, o mecanismo de "abertura" de portas acha-se atualmente incorporado em diversos ataques de vírus e Invasões, sendo agora um mecanismo agregado a essas invasões, para que o atacante consiga acesso às informações do computador invadido.

Algumas alterações maliciosas e esse programa foi colocado a serviço "do mal", pois, como um programa-cliente, permite abrir, durante uma conexão Internet, uma porta traseira de acesso (backdoor) na estação usuária, habilitando o invasor a controlar a máquina completamente – eliminando, copiando e criando arquivos, impedindo o uso de periféricos, avariando o acesso a determinados serviços, tendo acesso a acervos e informações sigilosas, etc.
Alguns desses programas atingiram níveis perigosos de sofisticação e foram utilizados para ataques a grandes instalações. A exemplo dos vírus, o mecanismo de "abertura" de portas acha-se atualmente incorporado em diversos ataques de vírus e invasões, sendo agora um mecanismo agregado a essas invasões, para que o atacante consiga acesso às informações do computador invadido.

Sugador de pacotes ("Packet Sniffer")

Programas e agentes (programas diminutos, que rodam em ambientes de pequeno porte e em redes, com poucos recursos) capturam

"pacotes" TCP/IP transmitidos em redes, interceptando-os. Nesse momento, cópias destes podem ser feitas, partes de transmissões interceptadas e eliminadas, impedindo a comunicação, etc.

Teoricamente, esses programas permitiriam que informações encaminhadas na Internet ou em redes diversas pudessem ser clonadas, copiadas e destruídas. O princípio também foi retirado de programas de suporte e auxílio ao usuário, levando a criar outra ferramenta de destruição de serviços.

Enchentes ("Flood")

É um tipo de ataque que objetiva solicitar todas as requisições disponíveis em um servidor, levando-o a não conseguir mais absorver o fluxo advindo dos usuários normais. O termo SYNFlood vem sendo aplicado ao tipo de ataque que envolve a manipulação dos sinais de sincronismo (chamados de SYN) no início do estabelecimento de uma conexão TCP/IP.

Dessa forma, a estação ficaria "em suspenso", aguardando uma mensagem de reconhecimento de conexão, que jamais chegará. Com muitas "esperas" desse tipo, um novo atendimento torna-se impossível ou a velocidade de atendimento normal cai para tempos inaceitáveis.

Dessa forma, muitos dos serviços de segurança disponíveis deixam de funcionar, incluindo os "rastreamentos" que permitem a identificação de segurança das fontes de origem de ataques.

Assusta saber que esse tipo de serviços é disponibilizado em sites da Internet com propagandas e links diversos, como se fosse um site comercial. Esse recurso objetiva que o número de IP de máquina conectada à rede não possa ser identificado. Dessa forma, muitos dos serviços de segurança disponíveis deixam de funcionar, incluindo os "rastreamentos" que permitem a identificação de segurança das fontes de origem de ataques.

Nas páginas consultadas, obviamente não incluídas, surpreendeu a existência de versões para sistemas operacionais diversos, informações do uso e patrocínio do uso dos softwares oferecidos. A tese de que se destinariam a pesquisas, experimentos ou outras funções mais nobres não procede, uma vez que, geralmente, as próprias páginas recomendavam seu uso maligno.

"Ping da Morte" (Ping of Death)

Recurso que consiste no envio de pacotes TCP/IP de tamanhos inválidos para servidores, levando-os ao travamento ou impedimento de trabalho. Esse recurso foi muito utilizado no início dos provimentos Internet no Brasil, para o impedimento de serviços. Atualmente, são bloqueados por boa parte dos sistemas básicos de segurança.

Exploração de "furos" em sistemas, servidores e clientes

Não param de ocorrer casos e informações (verídicas, em sua maioria, posto que reconhecidas pelos fornecedores) sobre mau funcionamento de programas desse tipo, que podem permitir aos invasores atuar da forma como quiserem.

Tomamos conhecimento, recentemente, do caso de um invasor que se aproveitou de um "furo" (mau funcionamento) de um servidor de impressão de um sistema Unix, que havia sido informado num arquivo de atualização, em versão posterior. O atacante pôs-se a procurar um sistema que funcionasse à base daquela versão do Unix, conseguindo encontrá-lo após alguma pesquisa. O "furo" consistia numa operação inválida que lhe permitia ter acesso a funções privativas do sistema operacional, ao alcance do super-usuário.

De posse dessas funções, sucessivamente, instalou ali um servidor de chat que visava a atender – às custas do processamento em máquina alheia – às suas conversas com amigos. O servidor, após muitos problemas de atendimento aos seus reais usuários, foi recuperado com a eliminação do programa de chat, reinstalado em seqüência pelo invasor. Na segunda desinstalação, este aproveitou novo acesso à máquina conectada para destruir arquivos e avariar a instalação do sistema de forma irrecuperável, levando a paradas do sistema e conseqüentes prejuízos.

A imprensa noticia constantemente que a versão X do servidor ou cliente Y possui uma falha de segurança – da qual um atacante ou invasor poderia servir-se para perpetrar seus crimes – reconhecida pelo fabricante, que já teria disponibilizado sua correção em seu site. Esse tipo de comportamento não deve ser visto como habitual. As questões de violação de segurança são críticas e como tais devem ser relevadas.

O acompanhamento e a manutenção da segurança patrimonial no tocante às informações e serviços de tecnologia da informação são responsabilidade dos profissionais de suporte e auditores de sistemas, que têm como prioridade de suas ações profissionais a garantia de funcionamento e propriedade de suas instalações.

Mostramos aqui, com a intenção de conscientizar e prevenir, diversos tipos de ataques promovidos hoje nos sistemas informatizados. Lamentavelmente, essa relação cresce dia após dia, dada a criatividade de potenciais criminosos que atuam numa nova esfera, a da propriedade da informação e de serviços associados que, senso comum, é hoje um dos maiores patrimônios da humanidade, quer nos negócios, quer na vida cotidiana. O acompanhamento e a manutenção da segurança patrimonial no tocante às informações e serviços de tecnologia da informação são responsabilidade dos profissionais de suporte e auditores de sistemas, que têm como prioridade de suas ações profissionais a garantia de funcionamento e propriedade de suas instalações. Porém, os cuidados na preservação e manutenção de acervos são problema afeto a todos, desde o operador, passando pelo usuário e chegando até mesmo aos projetistas de soluções de TI, que devem se preocupar com a segurança, incluindo-a como base em suas novas criações.

George Leal Jamil é engenheiro eletricista, mestre em Ciência da Computação, escritor, articulista, consultor nas áreas de ensino e tecnologia da informação, diretor da Sucesu-MG e professor da FACE-FUMEC.