Cartilha de Segurança para Internet
Parte I: Conceitos de Segurança

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, certificados digitais, engenharia social, vírus e *worm*, vulnerabilidade, *backdoor*, cavalo de tróia e ataques de negação de serviço. Os conceitos aqui apresentados são importantes para o entendimento de partes subseqüentes desta Cartilha.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 Segurança de Computadores

Um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade.

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Alguns exemplos de violações a cada um desses requisitos são:

Confidencialidade: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua Declaração de Imposto de Renda;

Integridade: alguém obtém acesso não autorizado ao seu computador e altera informações da sua Declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal;

Disponibilidade: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua Declaração de Imposto de Renda à Receita Federal.

1.1 Por que devo me preocupar com a segurança do meu computador?

Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de *e-mails*; armazenamento de dados, sejam eles pessoais ou comerciais, etc.

É importante que você se preocupe com a segurança de seu computador, pois você, provavelmente, não gostaria que:

- suas senhas e números de cartões de crédito fossem furtados;
- sua conta de acesso à Internet fosse utilizada por alguém não autorizado;
- seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por estranhos, etc.

1.2 Por que alguém iria querer invadir meu computador?

A resposta para esta pergunta não é simples. Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros. Alguns destes motivos podem ser:

- utilizar seu computador em alguma atividade ilícita, para esconder sua real identidade e localização;

- utilizar seu computador para lançar ataques contra outros computadores;
- utilizar seu disco rígido como repositório de dados;
- meramente destruir informações (vandalismo);
- disseminar mensagens alarmantes e falsas;
- ler e enviar *e-mails* em seu nome;
- propagar vírus de computador;
- furtar números de cartões de crédito e senhas bancárias;
- furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você;
- furtar dados do seu computador, como por exemplo informações do seu Imposto de Renda.

2 Senhas

Uma senha (*password*) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

Se você fornece sua senha para uma outra pessoa, esta poderá utilizá-la para se passar por você na Internet. Alguns dos motivos pelos quais uma pessoa poderia utilizar sua senha são:

- ler e enviar *e-mails* em seu nome;
- obter informações sensíveis dos dados armazenados em seu computador, tais como números de cartões de crédito;
- esconder sua real identidade e então desferir ataques contra computadores de terceiros.

Portanto, a senha merece consideração especial, afinal ela é de sua inteira responsabilidade.

2.1 O que não se deve usar na elaboração de uma senha?

O seu sobrenome, números de documentos, placas de carros, números de telefones e datas[1] deverão estar **fora** de sua lista de senhas. Esses dados são muito fáceis de se obter e qualquer pessoa tentaria utilizar este tipo de informação para tentar se autenticar como você.

Existem várias regras de criação de senhas, sendo que uma regra muito importante é **jamais** utilizar palavras que façam parte de dicionários. Existem *softwares* que tentam descobrir senhas combinando e testando palavras em diversos idiomas e geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.).

[1] Qualquer data que possa estar relacionada com você, como por exemplo a data de seu aniversário ou de familiares.

2.2 O que é uma boa senha?

Uma boa senha deve ter pelo menos oito caracteres[2] (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar.

Normalmente os sistemas diferenciam letras maiúsculas das minúsculas, o que já ajuda na composição da senha. Por exemplo, "`pAraleLepiPedo`" e "`paRalElePipEdo`" são senhas diferentes. Entretanto, são senhas fáceis de descobrir utilizando *softwares* para quebra de senhas, pois não possuem números e símbolos e contém muitas repetições de letras.

2.3 Como elaborar uma boa senha?

Quanto mais "bagunçada" for a senha melhor, pois mais difícil será descobrí-la. Assim, tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

Por exemplo, usando a frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "`!BqnsepC`" (o sinal de exclamação foi colocado no início para acrescentar um símbolo à senha). Senhas geradas desta maneira são fáceis de lembrar e são normalmente difíceis de serem descobertas.

Mas lembre-se: a senha "`!BqnsepC`" deixou de ser uma boa senha, pois faz parte desta Cartilha.

2.4 Quantas senhas diferentes devo usar?

Procure identificar o número de locais onde você necessita utilizar uma senha. Este número deve ser equivalente a quantidade de senhas **distintas** a serem mantidas por você. Utilizar senhas diferentes, uma para cada local, é extremamente importante, pois pode atenuar os prejuízos causados, caso alguém descubra uma de suas senhas.

Para ressaltar a importância do uso de senhas diferentes, imagine que você é responsável por realizar movimentações financeiras em um conjunto de contas bancárias e todas estas contas possuem a mesma senha. Então, procure responder as seguintes perguntas:

- Quais seriam as conseqüências se alguém descobrisse esta senha?
- E se elas fossem diferentes, uma para cada conta, caso alguém descobrisse uma das senhas, um possível prejuízo teria a mesma proporção?

[2] Existem serviços que permitem utilizar senhas maiores do que oito caracteres. Quanto maior for a senha, mais difícil será descobrí-la, portanto procure utilizar a maior senha possível.

2.5 Com que freqüência devo mudar minhas senhas?

Você deve trocar suas senhas regularmente, procurando evitar períodos muito longos. Uma sugestão é que você realize tais trocas a cada dois ou três meses.

Procure identificar se os serviços que você utiliza e que necessitam de senha, quer seja o acesso ao seu provedor, *e-mail*, conta bancária, ou outro, disponibilizam funcionalidades para alterar senhas e use regularmente tais funcionalidades.

Caso você não possa escolher sua senha na hora em que contratar o serviço, procure trocá-la com a maior urgência possível. Procure utilizar serviços em que você possa escolher a sua senha.

Lembre-se que trocas regulares são muito importantes para assegurar a integridade de suas senhas.

2.6 Quais os cuidados especiais que devo ter com as senhas?

De nada adianta elaborar uma senha bastante segura e difícil de ser descoberta, se ao usar a senha alguém puder vê-la. Existem várias maneiras de alguém poder descobrir a sua senha. Dentre elas, alguém poderia:

- observar o processo de digitação da sua senha;
- utilizar algum método de persuasão, para tentar convencê-lo a entregar sua senha (vide seção 5.1);
- capturar sua senha enquanto ela trafega pela rede.

Em relação a este último caso, existem técnicas que permitem observar dados, à medida que estes trafegam entre redes. É possível que alguém extraia informações sensíveis desses dados, como por exemplo senhas, caso não estejam criptografados (vide parte III desta Cartilha: Privacidade).

Portanto, alguns dos principais cuidados que você deve ter com suas senhas são:

- certifique-se de não estar sendo observado ao digitar a sua senha;
- não forneça sua senha para qualquer pessoa, em hipótese alguma;
- certifique-se que seu provedor disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

3 Certificado Digital

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.

Exemplos semelhantes a um certificado são o RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a pessoa e alguma autoridade (para estes exemplos, órgãos públicos) garantindo sua validade.

Algumas das principais informações encontradas em um certificado digital são:

- dados que identificam o dono (nome, número de identificação, estado, etc);
- nome da Autoridade Certificadora (AC) que emitiu o certificado (vide seção 3.1);
- o número de série do certificado;
- o período de validade do certificado;
- a assinatura digital da AC.

O objetivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas.

3.1 O que é Autoridade Certificadora (AC)?

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Os certificados digitais possuem uma forma de assinatura eletrônica da AC que o emitiu. Graças à sua idoneidade, a AC é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico".

3.2 Que exemplos podem ser citados sobre o uso de certificados?

Alguns exemplos típicos do uso de certificados digitais são:

- quando você acessa um *site* com conexão segura, como por exemplo o acesso à sua conta bancária pela Internet (vide parte IV desta Cartilha: Fraudes na Internet), é possível checar se o *site* apresentado é realmente da instituição que diz ser, através da verificação de seu certificado digital;
- quando você consulta seu banco pela Internet, este tem que assegurar-se de sua identidade antes de fornecer informações sobre a conta;
- quando você envia um *e-mail* importante, seu aplicativo de *e-mail* pode utilizar seu certificado para assinar "digitalmente" a mensagem, de modo a assegurar ao destinatário que o *e-mail* é seu e que não foi adulterado entre o envio e o recebimento.

A parte IV desta Cartilha (Fraudes na Internet) apresenta algumas medidas de segurança relacionadas ao uso de certificados digitais.

4 *Cookies*

Cookies são pequenas informações que os *sites* visitados por você podem armazenar em seu *browser*. Estes são utilizados pelos *sites* de diversas formas, tais como:

- guardar a sua identificação e senha quando você vai de uma página para outra;
- manter listas de compras ou listas de produtos preferidos em *sites* de comércio eletrônico;
- personalizar *sites* pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas;
- manter a lista das páginas vistas em um *site*, para estatística ou para retirar as páginas que você não tem interesse dos *links*.

A parte III desta Cartilha (Privacidade) apresenta alguns problemas relacionados aos *cookies*, bem como algumas sugestões para que se tenha maior controle sobre eles.

5 Engenharia Social

O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

5.1 Que exemplos podem ser citados sobre este método de ataque?

O primeiro exemplo apresenta um ataque realizado por telefone. Os outros dois exemplos apresentam casos onde foram utilizadas mensagens de *e-mail*.

Exemplo 1: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigí-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.

Exemplo 2: você recebe uma mensagem de *e-mail*, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um *site* da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Exemplo 3: você recebe uma mensagem *e-mail*, onde o remetente é o gerente ou o departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso à conta bancária e enviá-la para o atacante.

Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados nos exemplos procuram **induzir** o usuário a realizar alguma tarefa e o **sucesso** do ataque depende única e exclusivamente da **decisão** do usuário em fornecer informações sensíveis ou executar programas.

A parte IV desta Cartilha (Fraudes na Internet) apresenta algumas formas de se prevenir contra este tipo de ataque.

6 Vulnerabilidade

Vulnerabilidade é definida como uma falha no projeto ou implementação de um *software* ou sistema operacional, que quando explorada por um atacante resulta na violação da segurança de um computador.

Existem casos onde um *software* ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

A parte II desta Cartilha (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção) apresenta algumas formas de identificação de vulnerabilidades, bem como maneiras de prevenção e correção.

7 Vírus

Vírus é um programa capaz de infectar outros programas e arquivos de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que quando executado também executa o vírus, dando continuidade ao processo de infecção.

7.1 Como um vírus pode afetar um computador?

Normalmente o vírus tem controle total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de “feliz aniversário”, até alterar ou destruir programas e arquivos do disco.

7.2 Como o computador é infectado por um vírus?

Para que um computador seja infectado por um vírus, é preciso que de alguma maneira um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- abrir arquivos anexados aos *e-mails*;
- abrir arquivos do *Word*, *Excel*, etc;
- abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, ou de CD-ROM;
- esquecer um disquete no drive A: quando o computador é ligado;

Novas formas de infecção por vírus podem surgir. Portanto, é importante manter-se informado através de jornais, revistas e dos *sites* dos fabricantes de antivírus.

7.3 Um computador pode ser infectado por um vírus sem que se perceba?

Sim. Existem vírus que procuram permanecer **ocultos**, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Ainda existem outros tipos que permanecem inativos durante certos períodos, entrando em atividade em datas específicas.

7.4 O que é um vírus propagado por *e-mail*?

Um vírus propagado por *e-mail* (*e-mail borne virus*) normalmente é recebido como um arquivo anexado à uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado. Quando este tipo de vírus entra em ação, além de infectar arquivos e programas, envia cópias de si mesmo para todos os contatos encontrados nas listas de endereços de *e-mail* armazenadas no computador.

É importante ressaltar que este tipo específico de vírus não é capaz de se propagar automaticamente. O usuário precisa executar o arquivo anexado que contém o vírus, ou o programa de *e-mail* precisa estar configurado para auto-executar arquivos anexados.

7.5 O que é um vírus de macro?

Uma macro é um conjunto de comandos que são armazenados em alguns aplicativos, e utilizados para automatizar algumas tarefas repetitivas. Um exemplo seria, em um editor de textos, definir uma macro que contenha a seqüência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons de cinza.

Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros. Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir dai, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

Existem alguns aplicativos que possuem arquivos base (modelos) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será.

Arquivos nos formatos gerados pelo *Microsoft Word*, *Excel*, *Powerpoint* e *Access* são os mais suscetíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e PS são menos suscetíveis, mas isso não significa que não possam conter vírus.

8 *Worm*

Worm é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

8.1 Como um *worm* pode afetar um computador?

Geralmente o *worm* não tem como conseqüência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não que dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

9 *Backdoors*

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, a intenção do atacante é poder retornar ao computador comprometido sem ser notado.

A esses programas de retorno a um computador comprometido, utilizando-se serviços criados ou modificados para este fim, dá-se o nome de *Backdoor*.

9.1 Como é feita a inclusão de um *backdoor* em um computador?

A forma usual de inclusão de um *backdoor* consiste na adição de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente incluindo recursos que permitam acesso remoto (através da Internet).

Uma outra forma se dá através de pacotes de *software*, tais como o *BackOrifice* e *NetBus*, da plataforma Windows, conhecidos por disponibilizarem *backdoors* nos computadores onde são instalados.

9.2 A existência de um *backdoor* depende necessariamente de uma invasão?

Não. Alguns dos casos onde a existência de um *backdoor* não está associada a uma invasão são:

- instalação através de um cavalo de tróia (vide seção 10).
- inclusão como conseqüência da instalação e má configuração de um programa de administração remota;

Alguns fabricantes incluem/incluíam *backdoors* em seus produtos (*softwares*, sistemas operacionais), alegando necessidades administrativas. É importante ressaltar que estes casos constituem um séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que *backdoors* sejam incluídos por fabricantes conhecidos.

9.3 O uso de *backdoor* é restrito a um sistema operacional específico?

Não. *Backdoors* podem ser incluídos em computadores executando diversos sistemas operacionais, tais como Windows (por exemplo, 95/98, 2000, NT, XP), Unix (por exemplo, Linux, Solaris, FreeBSD, OpenBSD, AIX) e Mac OS.

10 Cavalo de Tróia

Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia".

Na informática, um Cavalo de Tróia (*Trojan Horse*) é um programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- alteração ou destruição de arquivos;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador.

10.1 Como um cavalo de tróia pode ser diferenciado de um vírus ou *worm*?

Por definição, o cavalo de tróia distingue-se de vírus e *worm*, por não se replicar, infectar outros arquivos, ou propagar cópias de si mesmo automaticamente.

Normalmente um cavalo de tróia consiste de um único arquivo que necessita ser explicitamente executado.

Podem existir casos onde um cavalo de tróia contenha um vírus ou *worm*. Mas mesmo nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*.

10.2 Como um cavalo de tróia se instala em um computador?

É necessário que o cavalo de tróia seja executado para que ele se instale em um computador. Geralmente um cavalo de tróia vem anexado a um *e-mail* ou está disponível em algum *site* na Internet.

É importante ressaltar que existem programas de *e-mail*, que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que qualquer arquivo (executável) anexado seja executado.

10.3 Que exemplos podem ser citados sobre programas contendo cavalos de tróia?

Exemplos comuns de cavalos de tróia são programas que você recebe ou obtém de um *site* e que **dizem** ser jogos ou protetores de tela. Enquanto estão sendo executados, este programas além de mostrar na tela uma mensagem como “Em que nível de dificuldade você quer jogar?”, ou apresentar todas aquelas animações típicas de um protetor de tela, podem ao mesmo tempo apagar arquivos ou formatar o disco rígido, enviar dados confidenciais para outro computador, instalar *backdoors*, ou alterar informações.

11 Negação de Serviço (*Denial of Service*)

Nos ataques de negação de serviço (DoS – *Denial of Service*) o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Exemplos deste tipo de ataque são:

- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível;
- tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários às suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*.

11.1 O que é DDoS?

DDoS (*Distributed Denial of Service*) constitui um ataque de negação de serviço distribuído, ou seja, **um conjunto** de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

11.2 Se uma rede ou computador sofrer um DoS, isto significa que houve uma invasão?

Não. O objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadí-los. É importante notar que, principalmente em casos de DDoS, computadores comprometidos podem ser utilizados para desferir os ataques de negação de serviço.

Um exemplo deste tipo de ataque ocorreu no início de 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos *sites* de algumas empresas de comércio eletrônico. Estas empresas não tiveram seus computadores comprometidos, mas sim ficaram impossibilitadas de vender seus produtos durante um longo período.