Cartilha de Segurança para Internet

Parte VIII: Códigos Maliciosos (*Malware*)

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte VIII: Códigos Maliciosos (*Malware*)

Esta parte da Cartilha aborda os conceitos e métodos de prevenção para diversos códigos maliciosos (*malwares*), que são programas especificamente desenvolvidos para executar ações danosas em um computador. Dentre eles serão discutidos vírus, cavalos de tróia, *spywares*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits*.

Versão 3.0 – Setembro de 2005
http://cartilha.cert.br/

Sumário

1 Vírus **4**
1.1 Como um vírus pode afetar um computador? . . . 4
1.2 Como o computador é infectado por um vírus? . . . 4
1.3 Um computador pode ser infectado por um vírus sem que se perceba? . . . 4
1.4 O que é um vírus propagado por *e-mail*? . . . 4
1.5 O que é um vírus de macro? . . . 5
1.6 Como posso saber se um computador está infectado? . . . 5
1.7 Existe alguma maneira de proteger um computador de vírus? . . . 5
1.8 O que é um vírus de telefone celular? . . . 6
1.9 Como posso proteger um telefone celular de vírus? . . . 6

2 Cavalos de Tróia **7**
2.1 Como um cavalo de tróia pode ser diferenciado de um vírus ou *worm*? . . . 7
2.2 Como um cavalo de tróia se instala em um computador? . . . 8
2.3 Que exemplos podem ser citados sobre programas contendo cavalos de tróia? . . . 8
2.4 O que um cavalo de tróia pode fazer em um computador? . . . 8
2.5 Um cavalo de tróia pode instalar programas sem o conhecimento do usuário? . . . 8
2.6 É possível saber se um cavalo de tróia instalou algo em um computador? . . . 8
2.7 Existe alguma maneira de proteger um computador dos cavalos de tróia? . . . 9

3 *Adware* e *Spyware* **9**
3.1 Que exemplos podem ser citados sobre programas *spyware*? . . . 10
3.2 É possível proteger um computador de programas *spyware*? . . . 10

4 *Backdoors* **11**
4.1 Como é feita a inclusão de um *backdoor* em um computador? . . . 11
4.2 A existência de um *backdoor* depende necessariamente de uma invasão? . . . 11
4.3 *Backdoors* são restritos a um sistema operacional específico? . . . 12
4.4 Existe alguma maneira de proteger um computador de *backdoors*? . . . 12

5 *Keyloggers* **12**
5.1 Que informações um *keylogger* pode obter se for instalado em um computador? . . . 12
5.2 Diversos *sites* de instituições financeiras utilizam teclados virtuais. Neste caso eu estou protegido dos *keyloggers*? . . . 13
5.3 Como é feita a inclusão de um *keylogger* em um computador? . . . 13
5.4 Como posso proteger um computador dos *keyloggers*? . . . 13

6 *Worms* **13**
6.1 Como um *worm* pode afetar um computador? . . . 14
6.2 Como posso saber se meu computador está sendo utilizado para propagar um *worm*? 14
6.3 Como posso proteger um computador de *worms*? . . . 14

7 *Bots e Botnets* **14**
7.1 Como o invasor se comunica com o *bot*? . . . 15
7.2 O que o invasor pode fazer quando estiver no controle de um *bot*? . . . 15
7.3 O que são *botnets*? . . . 15
7.4 Como posso saber se um *bot* foi instalado em um computador? . . . 15
7.5 Como posso proteger um computador dos *bots*? . . . 15

8 *Rootkits* **16**
8.1 Que funcionalidades um *rootkit* pode conter? 16
8.2 Como posso saber se um *rootkit* foi instalado em um computador? 17
8.3 Como posso proteger um computador dos *rootkits*? 17

Como Obter este Documento **18**

Nota de Copyright e Distribuição **18**

Agradecimentos **18**

1 Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Nesta seção, entende-se por computador qualquer dispositivo computacional passível de infecção por vírus. Computadores domésticos, *notebooks*, telefones celulares e PDAs são exemplos de dispositivos computacionais passíveis de infecção.

1.1 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.

1.2 Como o computador é infectado por um vírus?

Para que um computador seja infectado por um vírus, é preciso que 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, *pen drives*, CDs, DVDs, etc;
- ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele 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.

1.3 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.

1.4 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, ele infecta arquivos e programas e envia cópias de si mesmo para os contatos encontrados nas listas de endereços de *e-mail* armazenadas no computador do usuário.

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 leitor de *e-mails* precisa estar configurado para auto-executar arquivos anexados.

1.5 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 daí, 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 por programas da Microsoft, como o Word, Excel, Powerpoint e Access, são os mais suscetíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e *PostScript* são menos suscetíveis, mas isso não significa que não possam conter vírus.

1.6 Como posso saber se um computador está infectado?

A melhor maneira de descobrir se um computador está infectado é através dos programas antivírus[1].

É importante ressaltar que o antivírus e suas assinaturas devem estar **sempre atualizados**, caso contrário poderá **não** detectar os vírus mais recentes.

1.7 Existe alguma maneira de proteger um computador de vírus?

Sim. Algumas das medidas de prevenção contra a infecção por vírus são:

- instalar e manter atualizados um bom programa antivírus e suas assinaturas;
- desabilitar no seu programa leitor de *e-mails* a auto-execução de arquivos anexados às mensagens;

[1] Maiores detalhes sobre antivírus podem ser encontrados na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

- não executar ou abrir arquivos recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus;
- procurar utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou *PostScript*;
- procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.

1.8 O que é um vírus de telefone celular?

Um vírus de celular se propaga de telefone para telefone através da tecnologia *bluetooth*[2] ou da tecnologia MMS[3] (*Multimedia Message Service*). A infecção se dá da seguinte forma:

1. O usuário recebe uma mensagem que diz que seu telefone está prestes a receber um arquivo.
2. O usuário permite que o arquivo infectado seja recebido, instalado e executado em seu aparelho.
3. O vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente.

Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no telefone celular, mas podem ser especificamente projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho.

Depois de infectar um telefone celular, o vírus pode realizar diversas atividades, tais como: destruir/sobrescrever arquivos, remover contatos da agenda, efetuar ligações telefônicas, drenar a carga da bateria, além de tentar se propagar para outros telefones.

1.9 Como posso proteger um telefone celular de vírus?

Algumas das medidas de prevenção contra a infecção por vírus em telefones celulares são:

- mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário. Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
- não permita o recebimento de arquivos enviados por terceiros, mesmo que venham de pessoas conhecidas, salvo quando você estiver esperando o recebimento de um arquivo específico;
- fique atento às notícias veiculadas no *site* do fabricante do seu aparelho, principalmente àquelas sobre segurança;

[2] Mais detalhes sobre a tecnologia *bluetooth* podem ser encontrados na parte III: Privacidade.
[3] A definição deste termo pode ser encontrada no Glossário.

- aplique todas as correções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
- caso você tenha comprado uma aparelho usado, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como descrito no primeiro item, antes de inserir quaisquer dados.

Os fabricantes de antivírus têm disponibilizado versões para diversos modelos de telefones celulares. Caso você opte por instalar um antivírus em seu telefone, consulte o fabricante e verifique a viabilidade e disponibilidade de instalação para o modelo do seu aparelho. Lembre-se de manter o antivírus sempre atualizado.

2 Cavalos 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, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), 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:

- instalação de *keyloggers* ou *screenloggers* (vide seção 5);
- 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;
- alteração ou destruição de arquivos.

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

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

Normalmente um cavalo de tróia consiste em 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*.

2.2 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 leitores de *e-mails* que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que um arquivo anexado seja executado.

2.3 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 algum *site* e que **parecem ser** apenas cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, entre outros.

Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar *backdoors*, alterar informações, apagar arquivos ou formatar o disco rígido.

Existem também cavalos de tróia, utilizados normalmente em esquemas fraudulentos, que, ao serem instalados com sucesso, apenas exibem uma mensagem de erro.

2.4 O que um cavalo de tróia pode fazer em um computador?

O cavalo de tróia, na maioria das vezes, instalará programas para possibilitar que um invasor tenha controle total sobre um computador. Estes programas podem permitir que o invasor:

- tenha acesso e copie todos os arquivos armazenados no computador;
- descubra todas as senhas digitadas pelo usuário;
- formate o disco rígido do computador, etc.

2.5 Um cavalo de tróia pode instalar programas sem o conhecimento do usuário?

Sim. Normalmente o cavalo de tróia procura instalar, sem que o usuário perceba, programas que realizam uma série de atividades maliciosas.

2.6 É possível saber se um cavalo de tróia instalou algo em um computador?

A utilização de um bom programa antivírus (desde que seja atualizado freqüentemente) normalmente possibilita a detecção de programas instalados pelos cavalos de tróia.

É importante lembrar que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por um cavalo de tróia, principalmente se estes programas forem mais recentes que as assinaturas do seu antivírus.

2.7 Existe alguma maneira de proteger um computador dos cavalos de tróia?

Sim. As principais medidas preventivas contra a instalação de cavalos de tróia são semelhantes às medidas contra a infecção por vírus e estão listadas na seção 1.7.

Uma outra medida preventiva é utilizar um *firewall* pessoal. Alguns *firewalls* podem bloquear o recebimento de cavalos de tróia, como descrito na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

3 *Adware* e *Spyware*

Adware (*Advertising software*) é um tipo de *software* especificamente projetado para apresentar propagandas, seja através de um *browser*, seja através de algum outro programa instalado em um computador.

Em muitos casos, os *adwares* têm sido incorporados a *softwares* e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Um exemplo do uso legítimo de *adwares* pode ser observado na versão gratuita do *browser* Opera.

Spyware, por sua vez, é o termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Existem *adwares* que também são considerados um tipo de *spyware*, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Os *spywares*, assim como os *adwares*, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Seguem algumas funcionalidades implementadas em *spywares*, que podem ter relação com o uso legítimo ou malicioso:

- monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- alteração da página inicial apresentada no *browser* do usuário;
- varredura dos arquivos armazenados no disco rígido do computador;
- monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;
- instalação de outros programas *spyware*;
- monitoramento de teclas digitadas pelo usuário ou regiões da tela próximas ao clique do *mouse* (vide seção 5);

- captura de senhas bancárias e números de cartões de crédito;
- captura de outras senhas usadas em *sites* de comércio eletrônico.

É importante ter em mente que estes programas, na maioria das vezes, comprometem a privacidade do usuário e, pior, a segurança do computador do usuário, dependendo das ações realizadas pelo *spyware* no computador e de quais informações são monitoradas e enviadas para terceiros.

A seção 3.1 apresenta alguns exemplos de *spywares* usados de modo legítimo e de *spywares* maliciosos.

3.1 Que exemplos podem ser citados sobre programas *spyware*?

Alguns exemplos de utilização de programas *spyware* de modo legítimo são:

- uma empresa pode utilizar programas *spyware* para monitorar os hábitos de seus funcionários, desde que tal monitoramento esteja previsto em contrato ou nos termos de uso dos recursos computacionais da empresa;
- um usuário pode instalar um programa *spyware* para verificar se outras pessoas estão utilizando o seu computador de modo abusivo ou não autorizado.

Na maioria das vezes, programas *spyware* são utilizados de forma dissimulada e/ou maliciosa. Seguem alguns exemplos:

- existem programas cavalo de tróia que instalam um *spyware*, além de um *keylogger* ou *screenlogger*. O *spyware* instalado monitora todos os acessos a *sites* enquanto o usuário navega na Internet. Sempre que o usuário acessa determinados *sites* de bancos ou de comércio eletrônico, o *keylogger* ou *screenlogger* é ativado para a captura de senhas bancárias ou números de cartões de crédito;
- alguns *adwares* incluem componentes *spyware* para monitorar o acesso a páginas *Web* durante a navegação na Internet e, então, direcionar as propagandas que serão apresentadas para o usuário. Muitas vezes, a licença de instalação do *adware* não diz claramente ou omite que tal monitoramento será feito e quais informações serão enviadas para o autor do *adware*, caracterizando assim o uso dissimulado ou não autorizado de um componente *spyware*.

A seção 3.2 apresenta algumas formas de se prevenir a instalação de programas *spyware* em um computador.

3.2 É possível proteger um computador de programas *spyware*?

Existem ferramentas específicas, conhecidas como "anti-*spyware*", capazes de detectar e remover uma grande quantidade de programas *spyware*. Algumas destas ferramentas são gratuitas para uso pessoal e podem ser obtidas pela Internet (antes de obter um programa anti-*spyware* pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável).

Além da utilização de uma ferramenta anti-*spyware*, as medidas preventivas contra a infecção por vírus (vide seção 1.7) são fortemente recomendadas.

Uma outra medida preventiva é utilizar um *firewall* pessoal[4], pois alguns *firewalls* podem bloquear o recebimento de programas *spyware*. Além disso, se bem configurado, o *firewall* pode bloquear o envio de informações coletadas por estes programas para terceiros, de forma a amenizar o impacto da possível instalação de um programa *spyware* em um computador.

4 *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, também é intenção do atacante poder retornar ao computador comprometido sem ser notado.

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

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

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Uma outra forma é a instalação de pacotes de *software*, tais como o *BackOrifice* e *NetBus*, da plataforma Windows, utilizados para administração remota. Se mal configurados ou utilizados sem o consentimento do usuário, podem ser classificados como *backdoors*.

4.2 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 2).
- 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 uma séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que *backdoors* sejam incluídos por fabricantes conhecidos.

[4] Mais informações podem ser obtidas na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

4.3 *Backdoors* são restritos a um sistema operacional específico?

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

4.4 Existe alguma maneira de proteger um computador de *backdoors*?

Embora os programas antivírus não sejam capazes de descobrir *backdoors* em um computador, as medidas preventivas contra a infecção por vírus (seção 1.7) são válidas para se evitar algumas formas de instalação de *backdoors*.

A idéia é que você **não** execute programas de procedência duvidosa ou desconhecida, sejam eles recebidos por *e-mail*, sejam obtidos na Internet. A execução de tais programas pode resultar na instalação de um *backdoor*.

Caso você utilize algum programa de administração remota, certifique-se de que ele esteja bem configurado, de modo a evitar que seja utilizado como um *backdoor*.

Uma outra medida preventiva consiste na utilização de um *firewall* pessoal[5]. Apesar de não eliminarem os *backdoors*, se bem configurados, podem ser úteis para amenizar o problema, pois podem barrar as conexões entre os invasores e os *backdoors* instalados em um computador.

Também é importante visitar constantemente os *sites* dos fabricantes de *softwares* e verificar a existência de novas versões ou *patches* para o sistema operacional ou *softwares* instalados em seu computador.

Existem casos onde a disponibilização de uma nova versão ou de um *patch* está associada à descoberta de uma vulnerabilidade em um *software*, que permite a um atacante ter acesso remoto a um computador, de maneira similar ao acesso aos *backdoors*.

5 *Keyloggers*

Keylogger é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

5.1 Que informações um *keylogger* pode obter se for instalado em um computador?

Um *keylogger* pode capturar e armazenar as teclas digitadas pelo usuário. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou *Internet Banking*. Normal-

[5] Mais informações podem ser obtidas na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

mente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

5.2 Diversos *sites* de instituições financeiras utilizam teclados virtuais. Neste caso eu estou protegido dos *keyloggers*?

As instituições financeiras desenvolveram os teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de usuários. Então, foram desenvolvidas formas mais avançadas de *keyloggers*, também conhecidas como *screenloggers*, capazes de:

- armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou
- armazenar a região que circunda a posição onde o *mouse* é clicado.

De posse destas informações um atacante pode, por exemplo, descobrir a senha de acesso ao banco utilizada por um usuário.

5.3 Como é feita a inclusão de um *keylogger* em um computador?

Normalmente, o *keylogger* vem como parte de um programa *spyware* (veja a seção 3) ou cavalo de tróia (veja a seção 2). Desta forma, é necessário que este programa seja executado para que o *keylogger* se instale em um computador. Geralmente, tais programas vêm anexados a *e-mails* ou estão disponíveis em *sites* na Internet.

Lembre-se que existem programas leitores de *e-mails* 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 anexado seja executado.

5.4 Como posso proteger um computador dos *keyloggers*?

Para se evitar a instalação de um *keylogger*, as medidas são similares àquelas discutidas nas seções de vírus (1.7), cavalo de tróia (2.7), *worm* (6.3), *bots* (7.5) e na parte IV: Fraudes na Internet.

6 *Worms*

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** embute cópias de si mesmo em outros programas ou arquivos e **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.

6.1 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 quer 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.

6.2 Como posso saber se meu computador está sendo utilizado para propagar um *worm*?

Detectar a presença de um *worm* em um computador não é uma tarefa fácil. Muitas vezes os *worms* realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *worms* e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

Portanto, o melhor é evitar que seu computador seja utilizado para propagá-los (vide seção 6.3).

6.3 Como posso proteger um computador de *worms*?

Além de utilizar um bom antivírus, que permita detectar e até mesmo evitar a propagação de um *worm*, é importante que o sistema operacional e os *softwares* instalados em seu computador não possuam vulnerabilidades.

Normalmente um *worm* procura explorar alguma vulnerabilidade disponível em um computador, para que possa se propagar. Portanto, as medidas preventivas mais importantes são aquelas que procuram evitar a existência de vulnerabilidades, como discutido na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

Uma outra medida preventiva é ter instalado em seu computador um *firewall* pessoal[6]. Se bem configurado, o *firewall* pessoal pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível em seu computador ou, em alguns casos, mesmo que o *worm* já esteja instalado em seu computador, pode evitar que explore vulnerabilidades em outros computadores.

7 *Bots e Botnets*

De modo similar ao *worm* (seção 6), o *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

[6] Mais informações podem ser obtidas na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

7.1 Como o invasor se comunica com o *bot*?

Normalmente, o *bot* se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas para este canal. O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*. Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

7.2 O que o invasor pode fazer quando estiver no controle de um *bot*?

Um invasor, ao se comunicar com um *bot*, pode enviar instruções para que ele realize diversas atividades, tais como:

- desferir ataques na Internet;
- executar um ataque de negação de serviço (detalhes na parte I: Conceitos de Segurança);
- furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
- enviar *e-mails* de *phishing* (detalhes na parte IV: Fraudes na Internet);
- enviar *spam*.

7.3 O que são *botnets*?

Botnets são redes formadas por computadores infectados com *bots*. Estas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

7.4 Como posso saber se um *bot* foi instalado em um computador?

Identificar a presença de um *bot* em um computador não é uma tarefa simples. Normalmente, o *bot* é projetado para realizar as instruções passadas pelo invasor sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *bots*, isto nem sempre é possível. Portanto, o melhor é procurar evitar que um *bot* seja instalado em seu computador (vide seção 7.5).

7.5 Como posso proteger um computador dos *bots*?

Da mesma forma que o *worm*, o *bot* é capaz de se propagar automaticamente, através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador.

Portanto, a melhor forma de se proteger dos *bots* é manter o sistema operacional e os *softwares* instalados em seu computador sempre atualizados e com todas as correções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

A utilização de um bom antivírus, mantendo-o sempre atualizado, também é importante, pois em muitos casos permite detectar e até mesmo evitar a propagação de um *bot*. Vale lembrar que o antivírus só será capaz de detectar *bots* conhecidos.

Outra medida preventiva consiste em utilizar um *firewall* pessoal[7]. Normalmente, os *firewalls* pessoais não eliminam os *bots*, mas, se bem configurados, podem ser úteis para amenizar o problema, pois podem barrar a comunicação entre o invasor e o *bot* instalado em um computador.

Podem existir outras formas de propagação e instalação de *bots* em um computador, como por exemplo, através da execução de arquivos anexados a *e-mails*. Portanto, as medidas apresentadas na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção também são fortemente recomendadas.

8 *Rootkits*

Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkit*.

É muito importante ficar claro que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para mantê-lo. Isto significa que o invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

8.1 Que funcionalidades um *rootkit* pode conter?

Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:

- programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc;
- *backdoors* (vide seção 4), para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
- programas para remoção de evidências em arquivos de *logs*;
- *sniffers*[8], para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- *scanners*[9], para mapear potenciais vulnerabilidades em outros computadores;

[7] Mais informações podem ser obtidas na parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.
[8] A definição de *sniffer* pode ser encontrada no Glossário.
[9] A definição de *scanner* pode ser encontrada no Glossário.

- outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

8.2 Como posso saber se um *rootkit* foi instalado em um computador?

Existem programas capazes de detectar a presença de um grande número de *rootkits*, mas isto não quer dizer que são capazes de detectar todos os disponíveis (principalmente os mais recentes). Alguns destes programas são gratuitos e podem ser obtidos pela Internet (antes de obter um programa para a detecção de *rootkits* pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável).

Como os *rootkits* são projetados para ficarem ocultos, ou seja, não serem detectados pelo responsável ou pelos usuários de um computador, sua identificação é, na maioria das vezes, uma tarefa bem difícil. Deste modo, o melhor é procurar evitar que um *rootkit* seja instalado em seu computador (vide seção 8.3).

8.3 Como posso proteger um computador dos *rootkits*?

Apesar de existirem programas específicos para a detecção de *rootkits*, a melhor forma de se proteger é manter o sistema operacional e os *softwares* instalados em seu computador sempre atualizados e com todas as correções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

Desta forma, você pode evitar que um atacante consiga invadir seu computador, através da exploração de alguma vulnerabilidade, e instalar um *rootkit* após o comprometimento.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. 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@cert.br.

Nota de *Copyright* e Distribuição

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.