casa do concurseiro
sinta-se em casa para estudar conosco

# Informática

## Pragas Virtuais

Professor Márcio Hunecke

## PRAGAS VIRTUAIS

**Malware, ou praga virtual** é todo e qualquer *software* que tem objetivos maliciosos. Em *malware*, se incluem todos os ***trojans,* vírus e *spywares***.

Esse grupo é muito genérico e é mais recomendado usar um dos grupos mais específicos como os citados. Na maioria das vezes, ***malware*** será apenas tratado como um grupo que engloba *spywares* e *adware*.

As principais áreas são as seguintes:

**(Textos retirados do site: http://cartilha.cert.br. Recomendo o acesso a essa cartilha para mais informações sobre segurança na Internet e sobre créditos e licença).**

### VÍRUS


Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de e-mail.

Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen-drives.*

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

**Vírus propagado por e-mail:** recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados

**Vírus de script:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

**Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o *Microsoft Office* (*Excel*, *Word* e *PowerPoint*, entre outros).

**Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (*Multimedia Message Service*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

## WORM

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


Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

*Worms* são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

## BACKDOORS

*Backdoor* é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

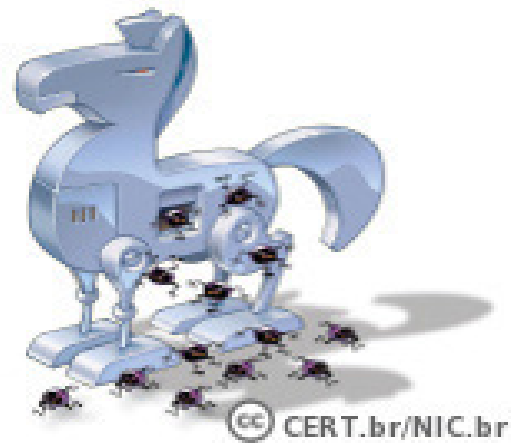

Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

## CAVALO DE TRÓIA




Cavalo de troia[1], trojan ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de trojans são programas que você recebe ou obtém desites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

[1] O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. 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 Troia.

## COMO UM CAVALO DE TRÓIA PODE SER DIFERENCIADO DE UM VÍRUS OU DE UM WORM?

Por definição, o cavalo de tróia distingue-se de vírus e de worm por não se replicar, infectaroutros 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.

## SPYWARE

*Spyware* é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.


Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

**Legítimo:** quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

**Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:


**Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a umsite específico de comércio eletrônico ou de Internet Banking.


**Screenlogger:** similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de *Internet Banking.*

## ADWARE

Projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.


## *Bot e botnet*

*Bot* é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.

Um computador infectado por um bot costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de e-mails e o utiliza para o envio de *spam*.

*Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Quanto mais zumbis participarem da botnet mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma *botnet:*

**a)** Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;

**b)** os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;

**c)** quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;

**d)** os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;

**e)** quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

## Ransomware

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é feito via bitcoins.

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam:

- através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link.
- explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

**O mais importante é evitar ser infectado!!!**

## SPANS

São e-mails enviados em massa sem autorização. Geralmente usados em: propagandas, correntes de fé, falsas ideologias, ajuda a outrem, entre muitos.

## HOAXES (brincadeiras)

São boatos espalhados por e-mail que servem para assustar o usuário de computador. Uma mensagem no e-mail alerta para um novo vírus totalmente destrutivo, nunca visto anteriormente, que está circulando na rede e que infectará o microcomputador do destinatário enquanto a mensagem estiver sendo lida ou quando o usuário clicar em determinada tecla ou link. Quem cria a mensagem hoax, normalmente, costuma dizer que a informação partiu de uma empresa confiável como IBM e Microsoft e que tal vírus poderá danificar a máquina do usuário. Desconsidere a mensagem.

## Phishing SCAM

O phishing online (pronuncia-se fíchin) é uma maneira de enganar os usuários de computador para que eles revelem informações pessoais ou financeiras através de uma mensagem de email ou site fraudulento. Um scam típico de phishing online começa com uma mensagem de email que parece uma nota oficial de uma fonte confiável como um banco, uma empresa de cartão de crédito ou um comerciante online de boa reputação. No email, os destinatários são direcionados a um site fraudulento em que são instruídos a fornecer suas informações pessoais, como número de conta ou senha. Em seguida, essas informações são geralmente usadas para o roubo de identidade.

## Antivírus

Origem: Wikipédia, a enciclopédia livre.

Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar vírus de computador.

## Métodos de identificação

**'Escaneamento de vírus conhecidos'** – Quando um novo vírus é descoberto seu código é desmontado e é separado um grupo de caracteres (uma *string*) que não é encontrada em outros softwares não maliciosos. Tal string passa a identificar esse vírus, e o antivírus a utiliza para ler cada arquivo do sistema (da mesma forma que o sistema operacional), de forma que quando a encontrar em algum arquivo, emite uma mensagem ao usuário ou apaga o arquivo automaticamente.

**'Sensoriamento heurístico'** – O segundo passo é a análise do código de cada programa em execução quando usuário solicita um escaneamento. Cada programa é varrido em busca de instruções que não são executadas por programas usuais, como a modificação de arquivos executáveis. É um método complexo e sujeito a erros, pois algumas vezes um executável precisa gravar sobre ele mesmo, ou sobre outro arquivo, dentro de um processo de reconfiguração, ou atualização, por exemplo. Portanto, nem sempre o aviso de detecção é confiável.

**'Checagem de Integridade'** – Checagem de integridade cria um banco de dados, com o registro dos dígitos verificadores de cada arquivo existente no disco, para comparações posteriores. Quando for novamente feita esta checagem, o banco de dados é usado para certificar que nenhuma alteração seja encontrada nesses dígitos verificadores. Caso seja encontrado algum desses dígitos diferentes dos gravados anteriormente, é dado o alarme da possível existência de um arquivo contaminado.

Os antivírus são programas que procuram por outros programas (os vírus) e/ou os barram, por isso, nenhum antivírus é totalmente seguro o tempo todo, e existe a necessidade de sua manutenção (atualização) e, antes de tudo, fazer sempre uso do backup para proteger-se realmente contra perda de dados importantes.

## Antispyware

Origem: Wikipédia, a enciclopédia livre.

Os *AntiSpywares* são programas cujo objetivo é tentar eliminar do sistema, através de uma varredura, *spywares*, *adwares*, *keyloggers*, *trojans* e outros *malwares*. As funções destes programas são semelhantes aos do antivírus, embora ele sempre deve ter cuidado para não confundi-los.

Exemplo de programas *antispyware*: *Windows Defender*, *Spybot*, *Spyware Terminator*, *Ad-Aware, Spy Sweeper.*

## Firewall

*Origem: Wikipédia, a enciclopédia livre.*

Um *firewall* é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O *firewall* pode ser do tipo filtros de pacotes, proxy de aplicações, etc. Os *firewalls* são geralmente associados a redes TCP/IP.

Este dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos normalmente é chamado de "*appliance*". A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.