

Conceitos relativos à proteção e segurança

Códigos Maliciosos (Malware)

Código malicioso ou Malware (Malicious Software) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

Na literatura de segurança o termo malware também é conhecido por “software malicioso”.

Alguns exemplos de malware são:

- vírus;
 - worms e bots;
 - backdoors;
 - cavalos de tróia;
 - keyloggers e outros programas spyware;
-

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 a suas caixas de correio no servidor de e-mail ou ao servidor Web.
-

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.

Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizada pelos métodos de criptografia para codificar e decodificar mensagens.

O que é criptografia de chave única?

A criptografia de chave única utiliza a mesma chave tanto para codificar quanto para decodificar mensagens. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade

de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.

O que é criptografia de chaves pública e privada?

A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Veja o exemplo, onde José e Maria querem se comunicar de maneira sigilosa. Então, eles terão que realizar os seguintes procedimentos:

1. José codifica uma mensagem utilizando a chave pública de Maria, que está disponível para o uso de qualquer pessoa;
 2. Depois de criptografada, José envia a mensagem para Maria, através da Internet;
 3. Maria recebe e decodifica a mensagem, utilizando sua chave privada, que é apenas de seu conhecimento;
 4. Se Maria quiser responder a mensagem, deverá realizar o mesmo procedimento, mas utilizando a chave pública de José.
-

O que é assinatura digital?

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

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 digital são o CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa e a autoridade (para estes exemplos, órgãos públicos) que garante 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;
- o número de série e 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.

Firewalls

Os firewalls são dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso entre redes de computadores.

Um tipo específico é o firewall pessoal, que é um software ou programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet.

Como o firewall pessoal funciona?

Se alguém ou algum programa suspeito tentar se conectar ao seu computador, um firewall bem configurado entra em ação para bloquear tentativas de invasão, podendo barrar também o acesso a backdoors, mesmo se já estiverem instalados em seu computador.

Alguns programas de firewall permitem analisar continuamente o conteúdo das conexões, filtrando vírus de e-mail, cavalos de tróia e outros tipos de malware, antes mesmo que os antivírus entrem em ação.

Também existem pacotes de firewall que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

Cavalos de Tróia

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.

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 no programa de troca instantânea de mensagens MSN Messenger.

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;
- 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.

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.

Keyloggers

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

Screenloggers

Forma avançada de keylogger, capaz 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.

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.

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.

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.

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.

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.

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.

Quais são os tipos de vírus?

Existem atualmente 14 categorias de vírus de computador. Vejam a seguir quais são os tipos de vírus e suas características:

Tipo	Característica
Arquivo	Vírus que anexa ou associa seu código a um arquivo. Geralmente, esse tipo de praga adiciona o código a um arquivo de programa normal ou sobrescreve o arquivo. Ele costuma infectar arquivos executáveis do Windows, especialmente .com e .exe, e não age diretamente sobre arquivos de dados. Para que seu poder destrutivo tenha efeito, é necessário que os arquivos contaminados sejam executados.
Alarme falso	Não causa dano real ao computador, mas consome tempo de conexão à Internet ao levar o usuário a enviar o alarme para o maior número de pessoas possível. Enquadra-se na categoria de <u>vírus-boato e cartas-corrente</u> .
Backdoor	Como o próprio nome diz, é um vírus que permitem que hackers controlem o micro infectado pela "porta de trás". Normalmente, os backdoors vêm embutidos em arquivos recebidos por e-mail ou baixados da rede. Ao executar o arquivo, o usuário libera o vírus, que abre uma porta da máquina para que o autor do programa passe a controlar a máquina de modo completo ou restrito.
Boot	Vírus que se infecta na área de inicialização dos disquetes e de discos rígidos. Essa área é onde se encontram arquivos essenciais ao sistema. Os vírus de boot costumam ter alto poder de destruição, impedindo, inclusive, que o usuário entre no micro.
Cavalo de Tróia (Trojan)	São programas aparentemente inofensivos que trazem embutidos outro programa (ou vírus) maligno.
Encriptados	Tipo recente que, por estarem codificados, dificultam a ação dos antivírus.
Hoax	Vírus boato. Mensagens que geralmente chegam por e-mail alertando o usuário sobre um vírus mirabolante, altamente destrutivo.
Macro	Tipo de vírus que infecta as macros (códigos executáveis utilizados em processadores de texto e planilhas de cálculo para automatizar tarefas) de documentos, desabilitando funções como Salvar, Fechar e Sair.
Multipartite	Vírus que infectam registro mestre de inicialização, trilhas de boot e arquivos
Mutante	Vírus programado para dificultar a detecção por antivírus. Ele se altera a cada execução do arquivo contaminado
Polimórfico	Varição mais inteligente do vírus mutante. Ele tenta dificultar a ação dos antivírus ao mudar sua estrutura interna ou suas técnicas de codificação.
Programa	Infectam somente arquivos executáveis, impedindo, muitas vezes, que o usuário ligue o micro.
Script	Vírus programado para executar comandos sem a interação do usuário. Há duas categorias de vírus script: a VB, baseada na linguagem de programação, e a JS, baseada em JavaScript. O vírus script pode vir embutido em imagens e em arquivos com extensões estranhas, como .vbs.doc, vbs.xls ou js.jpg
Stealth	Vírus "invisível" que usa uma ou mais técnicas para evitar detecção. O stealth pode redirecionar indicadores do sistema de modo a infectar um arquivo sem necessariamente alterar o arquivo infectado.

Spam

Spam é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciado como UCE (do inglês *Unsolicited Commercial E-mail*).

Boatos

Boatos (*hoaxes*) são *e-mails* que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Dentre os diversos boatos típicos, que chegam às caixas postais de usuários conectados à Internet, podem-se citar as correntes, pirâmides, mensagens sobre pessoas que estão prestes a morrer de câncer, entre outras.

Histórias deste tipo são criadas não só para espalhar desinformação pela Internet, mas também para outros fins maliciosos.

Phishing

O que é phishing e que situações podem ser citadas sobre este tipo de fraude?

Phishing, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A subseções a seguir apresentam cinco situações envolvendo *phishing*, que vêm sendo utilizadas por fraudadores na Internet. Observe que existem variantes para as situações apresentadas. Além disso, novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Pharming

O Pharming é uma técnica que utiliza o seqüestro ou a "contaminação" do DNS (Domain Name Server) para levar os usuários a um site falso, alterando o DNS do site de destino. O sistema também pode redirecionar os usuários para sites autênticos através de proxies controlados pelos phishers, que podem ser usados para monitorar e interceptar a digitação.

Os sites falsificados coletam números de cartões de crédito, nomes de contas, senhas e números de documentos. Isso é feito através da exibição de um pop-up para roubar a informação antes de levar o usuário ao site real. O programa mal-intencionado usa um certificado auto-assinado para fingir a autenticação e induzir o usuário a acreditar nele o bastante para inserir seus dados pessoais no site falsificado.

Outra forma de enganar o usuário é sobrepor a barra de endereço e status de navegador para induzi-lo a pensar que está no site legítimo e inserir suas informações.

Os phishers utilizam truques para instalar programas criminosos nos PCs dos consumidores e roubar diretamente as informações. Na maioria dos casos, o usuário não sabe que está infectado, percebendo apenas uma ligeira redução na velocidade do computador ou falhas de funcionamento atribuídas a vulnerabilidades normais de software. Um software de segurança é uma ferramenta necessária para evitar a instalação de programas criminosos se o usuário for atingido por um ataque.

Alguns veículos de divulgação descrevem Pharming como um tipo específico de Phishing.

Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em <http://cartilha.cert.br/>.

Sugestões de programas:

Antivírus:

AVG (Free Edition) – Freeware

Avast! – Freeware

Antispyware:

Spybot Search and Destroy – Freeware

AD-aware SE Personal Edition 2007 – Freeware

Firewall:

ZoneAlarm Free – Freeware

Sygate Personal Firewall – Freeware

Antispam:

Agnitum Spam Terrier – Freeware

SafestMail 3.0 AntiSpam (Freeware Edition) – Freeware

Obs: Todos os programas são facilmente encontrados no site <http://www.superdownloads.com.br>