Comitê Gestor da Internet no Brasil

Cartilha de Segurança para Internet

Glossário

Versão 3.1
2006

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

Cartilha de Segurança para Internet

Glossário

Versão 3.1 – Outubro de 2006
http://cartilha.cert.br/

Glossário

802.11 Refere-se a um conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

AC Veja Autoridade certificadora.

ADSL Do Inglês ***A**symmetric **D**igital **S**ubscriber **L**ine*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Adware Do Inglês ***Ad**vertising Soft**ware***. *Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

Antivírus Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

AP Do Inglês ***A**ccess **P**oint*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Artefato De forma geral, artefato é qualquer informação deixada por um invasor em um sistema comprometido. Pode ser um programa ou *script* utilizado pelo invasor em atividades maliciosas, um conjunto de ferramentas usadas pelo invasor, *logs* ou arquivos deixados em um sistema comprometido, a saída gerada pelas ferramentas do invasor, etc.

Assinatura digital Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Atacante Pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

Autoridade certificadora 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.

Backdoor Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Banda Veja Largura de banda.

Bandwidth Veja Largura de banda.

Bluetooth Termo que se refere a uma tecnologia de rádio-freqüência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

Boato *E-mail* que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta 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.

Bot Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc.

Botnets Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc.

Cable modem *Modem* projetado para operar sobre linhas de TV a cabo.

Cavalo de tróia
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.

Certificado digital
Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Veja também Assinatura digital.

Código malicioso
Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

Comércio eletrônico
Também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da Internet.

Comprometimento
Veja Invasão.

Conexão segura
Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

Correção de segurança
Correção especificamente desenvolvida para eliminar falhas de segurança em um *software* ou sistema operacional.

Criptografia Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

DDoS Do Inglês ***D**istributed **D**enial **o**f **S**ervice*. 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. Veja Negação de serviço.

DNS Do Inglês ***D**omain **N**ame **S**ystem*. Serviço que traduz nomes de domínios para endereços IP e vice-versa.

DoS Do Inglês ***D**enial **o**f **S**ervice*. Veja Negação de serviço.

E-commerce Veja Comércio eletrônico.

Endereço IP Este endereço é um número único para cada computador conectado à Internet, composto por uma seqüência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

Engenharia social
Método de ataque onde uma pessoa 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.

Exploit Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.

Falsa identidade
Ato onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

Firewall Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

***Firewall* pessoal**
Software ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet. É um tipo específico de *firewall*.

GnuPG Conjunto de programas gratuito e de código aberto, que implementa criptografia de chave única, de chaves pública e privada e assinatura digital.

GPG Veja GnuPG.

Harvesting Técnica utilizada por *spammers*, que consiste em varrer páginas *Web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

Hoax Veja Boato.

HTML Do Inglês ***H**yper**T**ext **M**arkup **L**anguage*. Linguagem universal utilizada na elaboração de páginas na Internet.

HTTP Do Inglês ***H**yper**T**ext **T**ransfer **P**rotocol*. Protocolo usado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o *browser*).

HTTPS Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

Identity theft Veja Falsa identidade.

IDS Do Inglês ***I**ntrusion **D**etection **S**ystem*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IEEE Acrônimo para *Institute of Electrical and Electronics Engineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletro-eletrônicos.

Invasão Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP Veja Endereço IP.

Keylogger Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

Largura de banda Quantidade de dados que podem ser transmitidos em um canal de comunicação, em um determinado intervalo de tempo.

Log Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

Malware Do Inglês ***Mal**icious soft**ware*** (*software* malicioso). Veja Código malicioso.

MMS Do Inglês ***M**ultimedia **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem Dispositivo que permite o envio e recebimento de dados utilizando as linhas telefônicas.

Negação de serviço Atividade maliciosa onde o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Número IP Veja Endereço IP.

Opt-in Regra de envio de mensagens que define que é proibido mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário. Veja também *Soft opt-in*.

Opt-out Regra de envio de mensagens que define que é permitido mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P Acrônimo para *peer-to-peer*. Arquitetura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, onde alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um

usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.

Password Veja Senha.

Patch Veja Correção de segurança.

PGP Do Inglês ***P**retty **G**ood **P**rivacy*. Programa que implementa criptografia de chave única, de chaves pública e privada e assinatura digital. Possui versões comerciais e gratuitas. Veja também GnuPG.

Phishing Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Porta dos fundos Veja *Backdoor*.

Proxy Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Rede sem fio Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Rootkit Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar 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 manter o acesso privilegiado em um computador previamente comprometido.

Scam Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*.

Scanner Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screenlogger 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. Veja também *Keylogger*.

Senha Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Site Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

SMS Do Inglês ***S**hort **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

Sniffer Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Soft opt-in Regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Desta forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* deste remetente. Veja *Opt-in*.

Spam 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 referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*).

Spammer Pessoa que envia *spam*.

Spyware 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. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

SSH Do Inglês ***S**ecure **Sh**ell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

SSID Do Inglês ***S**ervice **S**et **Id**entifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

SSL Do Inglês ***S**ecure **S**ockets **L**ayer*. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Veja também HTTPS.

Time zone Fuso horário.

Trojan horse Veja Cavalo de tróia.

UCE Do inglês ***U**nsolicited **C**ommercial **E**-mail*. Termo usado para se referir aos *e-mails* comerciais não solicitados.

URL Do Inglês **U**niversal **R**esource **L**ocator. Seqüência de caracteres que indica a localização de um recurso na Internet, como por exemplo, http://cartilha.cert.br/.

Vírus 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.

VPN Do Inglês *Virtual Private Network*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Web bug Imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esta página *Web* ou mensagem de *e-mail*.

WEP Do Inglês *Wired Equivalent Privacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

Wi-Fi Do Inglês *Wireless Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless Veja Rede sem fio.

WLAN Do Inglês *Wireless Local-Area Network*. Refere-se a um tipo de rede que utiliza ondas de rádio de alta freqüência, ao invés de cabos, para a comunicação entre os computadores.

Worm 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.

WPA Do Inglês **W**i-Fi *Protected Access*. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Esta tecnologia foi projetada para, através de atualizações de *software*, operar com produtos Wi-Fi que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

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.

Licença de Uso da Cartilha

Agradecimentos

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