5.0 - Ataques Maliciosos, Ameaças e Vulnerabilidades

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

Ataques Maliciosos, Ameaças e Vulnerabilidades

Ataques Maliciosos, Ameaças e Vulnerabilidades

- Profissionais de segurança são responsáveis por proteger sistemas contra ameaças e por lidar com ataques maliciosos quando eles ocorrem.
- Uma das maneiras mais efetivas de proteger sistemas computacionais é garantir que as vulnerabilidades que existem em cada infraestrutura de TI não se transformem em algo mais sério.

Ataques Maliciosos, Ameaças e Vulnerabilidades

- O que proteger?
  - Em um palavara, você está tentando proteger **ativos**.
  - Um ativo é qualquer item que tenha valor. Ativos de uma organização podem incluir:
    - **TI e infraestrutura de rede** - Hardware, software e serviços.
    - **Propriedade Intelectual** - Dados confidenciais como patentes, código-fonte, fórmulas ou projetos de engenharia.
    - **Finanças e dados financeiros** - Contas bancárias, dados de cartão de crédito e de transações financeiras.
    - **Disponibilidade e produtividade de serviços** - A capacidade de serviços computacionais e de software em dar suporte à produtividade para humanos e máquinas.
    - **Reputação** - Conformidade corporativa e imagem da marca.

Ataques Maliciosos, Ameaças e Vulnerabilidades

- Quem é o invasor?
  - É comum na mídia o termo **hacker** estar associado a qualquer acusado de usar tecnologia para terrorismo, vandalismo, fraude, roubo de identidade, propriedade intelectual e outras formas de crime.
  - No entanto, na comunidade de computação, o termo hacker geralmente descreve um programador ou especialista técnico particularmente brilhantes, que se deleita em explorar e aprender sistemas computacionais. Por causa desse conflito, o termo é um tema controverso.

Ataques Maliciosos, Ameaças e Vulnerabilidades

- Para amenizar a confusão em torno do termo hacker, é comum utilizar estas categorias:
  - Hackers black-hat - Tenta quebrar a segurança de TI pelo desafio e para provar habilidade técnica. Geralmente procuram vulnerabilidades e falhas em sistemas, porém, não as divulgam.
  - Hackers white-hat - Ou hacker ético, é um profissional de segurança da informação ou de redes que usa diversas ferramentas de teste de penetração para descobrir vulnerabilidades e tentar corrigi-las.
  - Hackers gray-hat - Também chamados *wannabe*, possuem capacidade medianas e pode um dia se tornar um black-hat.

Ataques Maliciosos, Ameaças e Vulnerabilidades

- Já um **cracker** é alguém com intenção hostil, possui habilidades sofisticadas e pode estar interessado em ganho financeiro.
  - Cracker representam a maior ameaça a redes e a recursos de informação.
- Outro tipo de atacante é o **script kiddie**.
  - Pessoa com pouca ou nenhuma habilidade, que simplesmente segue instruções ou usa uma abordagem de livro de receita para executar um ataque sem entender totalmente o significado das etapas que está realizando.

Ferramentas de Ataque

- Indivíduos maliciosos utilizam uma séries de ferramentas de hardware e software para ajudar a desferir seus ataques. Essas ferramentas e técnicas podem incluir:
  - Programas para varredura (*scanner*) de vulnerabilidade.
  - Programa para varredura de porta.
  - Farejadores (*sniffers*).
  - Programa para captura de teclado (*keyloggers*)

Brecha de Segurança

- **Brecha de Segurança**
  - Qualquer evento que resulte em uma violação de qualquer um dos princípios de segurança é uma brecha de segurança.
  - Algumas propositalmente atrapalham serviços de sistema. Outras são acidentais e podem resultar de falhas em hardware ou software.
  - Independente de uma brecha de segurança ser acidental ou maliciosa, ela pode afetar a capacidade de uma organização de realizar negócios, bem como sua credibilidade.

Brecha de Segurança

- Atividades que podem causar uma brecha de segurança incluem:
  - Ataques de negação de serviço (*Denial of Service* - DoS).
  - Ataques de negação de serviço distribuído (*Distributed Denial of Service* - DDoS).
  - Comportamento inaceitável de navegador web.
  - Uso de *backdoor* para acessar recursos.
  - Modificações acidentais em dados.

Ataque de negação de serviço

- **Ataque de negação de serviço**
  - Resulta em usuários legítimos sem acesso a um recurso de sistema.
  - É uma tentativa coordenada de negar um serviço, fazendo com que um computador realize uma tarefa não produtiva. Essa atividade excessiva torna o sistema indisponível para realizar operações legítimas.
  - Quando um disco fica cheio, o sistema trava uma conta, um computador falha ou uma CPU reduz a velocidade, o resultado é negar serviço.

Ataque de negação de serviço

- Ataques de DoS geralmente são originados a partir de um único computador.
- Uma vez que detecte um ataque de DoS, você poderá impedi-lo com facilidade.
- Dois tipos comuns de ataques de DoS são:
  - **Ataques lógicos** - Usam falhas de software para arruinar ou atrapalhar seriamente o desempenho de servidores remotos. Você pode impedir muitos desses ataques instalando as correções mais recentes para manter seu software atualizado.
  - **Ataques de inundação** - Ataques de inundação comprometem a CPU, memória ou recursos de rede do computador-vítima, enviando grandes quantidade de solicitações inúteis para a máquina.

Ataque de negação de serviço

- Uma das melhores defesas contra ataques de DoS é usar software de sistema de prevenção de intrusos (*Intrusion Prevent System* - IPS) ou dispositivos para detectar e impedir o ataque.
- Software e dispositivos de sistema de detecção de intrusão (*Intrusion Detection System* - IDS) também podem detectar ataques de DoS e alertá-lo quando estiverem em progresso.
- Atacantes podem disparar ataques de DoS usando protocolos comuns da Internet, como TCP e ICMP.

Ataque de negação de serviço

- Uma das técnicas populares para desferir uma inundação de pacotes é uma **inundação de SYN** (*SYN Flood*).
  - SYN é um bit de controle do TCP usado para sincronizar números de sequência.
  - Em uma inundação SYN, o atacante envia um grande número de pacotes que solicitam conexões com o computador-vítima. Este registra cada solicitação e reserva um local para conexão em uma tabela local na memória e, então, envia uma confirmação de volta ao atacante.
  - Como o atacante nunca responde, o computador-vítima enche sua tabela de conexões que aguardam todas as confirmações de solicitação.

Ataque de negação de serviço distribuída

- **Ataque de negação de serviço distribuída**
  - Tipo de ataque de DoS que envolve inundar um ou mais computadores-alvo com solicitações falsas.
  - Diferem de ataques DoS normais em escopo. Em um ataque DDoS, atacantes sequestram centenas ou mesmo milhares de computadores na Internet, plantando agentes de ataque automatizados nesses sistemas.

Navegação web inaceitável

- **Navegação web inaceitável**
  - Descreve o uso de um navegador Web de maneira não aceitável.
  - Cada organização deve ter uma política de uso aceitável que estabeleça claramente qual comportamento é aceitável e qual não é.
  - Uso não aceitável pode incluir usuários não autorizados que procurem arquivos ou diretórios de armazenamento de dados e informações que não deveriam ler ou simplesmente usuários que visitem web sites proibidos.

Backdoor

- **Backdoor**
  - Desenvolvedores de software às vezes incluem métodos de acesso ocultos em seus programas, chamados **backdoors**, que dão aos desenvolvedores ou ao pessoal de suporte acesso fácil para um sistema, sem ter de lutar com controles de segurança.
  - Atacantes também podem comprometer um sistema ao instalar nele seu próprio backdoor e usá-lo para evitar controles que o administrador tenha preparado para proteger o sistema computacional.

Modificações de dados

- **Modificações de dados**
  - Problemas com a integridade de dados, incluindo modificações parciais e acidentais em dados e o armazenamento de valores de dados incorretos, também podem causar uma brecha de segurança.
  - Uma modificação incompleta pode ocorrer quando vários processos tentam atualizar dados sem observar restrições básicas de integridade de dados.
  - Outro exemplo é truncar dados porque o campo do registro não é grande o suficiente para mantê-los completos. Isso pode ocorrer com a maioria das linguagens de programação e poder ser difícil de detectar. Porém, os resultados podem ser significativos. A solução é validar os dados antes de armazená-los e garantir que seus programas cumpram regras de integridade de dados.

Desafios de Segurança Adicionais

- **Desafios de Segurança Adicionais**
  - Desafios adicionais para garantir comunicações salvas e seguras podem ter origem em spam, hoaxes, spyware e até mesmo informações locais armazenadas por navegadores web. Também é possível que haja uma combinação desses.

Spam

- **Spam**
  - Spam é uma mensagem de e-mail ou mensagens instantâneas indesejadas.
  - A maior parte contém anúncios comerciais.
  - Enviar spams custa muito pouco.
  - Processar grandes volumes de mensagens indesejadas é dispendioso. Além disso, força o usuário receptor a desperdiçar tempo administrativo em limpeza e monitoramento de mensagens recebidas.

Hoax

- **Hoax**
  - Um *hoax* (ou boato) é um ato com intenção de enganar ou defraudar o receptor.
  - Embora hoaxes não infectem sistemas automaticamente, como vírus ou cavalos de tróia, lidar com eles leva tempo. Na verdade você pode acabar gastando muito mais tempo refutando hoaxes que lidando com incidentes reais de vírus e cavalos de tróia.

Cookies

- **Cookies**
  - Um **cookie** é um arquivo com detalhes colhidos em visitas anteriores a um sítio web. Esses detalhes podem incluir o nome do usuário, informações pessoais e outros. Mais adiante, quando o usuário enviar uma solicitação ao servidor web, o servidor poderá acessar o cookie em vez de solicitar que o usuário forneça as informações novamente.
  - O problema com cookies é que eles armazenam informações em arquivos de texto claro. Isso significa que qualquer pessoa com acesso ao seu computador potencialmente poderá ler o conteúdo de seus cookies.

Vulnerabilidades e Ameaças

- **Vulnerabilidades e Ameaças**
  - Uma **ameaça** é qualquer ação que possa danificar um ativo. Uma **vulnerabilidade** é qualquer ponto fraco em um sistema que possibilite que uma ameaça cause danos a ele. Ameaças normalmente exploram uma ou mais vulnerabilidades conhecidas.
  - Você encontrará muitas vulnerabilidades em uma organização normal, a tabela a seguir lista algumas delas.

Vulnerabilidades e Ameaças

Domínio	**Vulnerabilidade Comum**
Domínio de usuário	Atividade maliciosa intencional Engenharia Social
Domínio de estação de trabalho	Acesso de usuário não autorizado Falhas em software instalado
Domínio de LAN	Acesso não autorizado à rede Transmitir dados privativos não criptografados
Domínio de LAN para WAN	Exposição de acesso não autorizado de recursos internos ao público Introdução de software malicioso
Domínio de WAN	Ataques de negação de serviço Transmitir dados privativos não criptografados
Domínio de acesso remoto	Ataques de força bruta sobre acesso e dados privativos Acesso remoto não autorizado a recursos
Domínio de sistema/aplicativo	Acesso físico ou lógico não autorizados a recursos Falhas em sistemas operacionais de servidor ou em software aplicativo

Vulnerabilidades e Ameaças

- Uma ameaça é significativa de um ponto de vista de segurança. As ameaças mais comuns, incluem:
  - Software malicioso
  - Falha de hardware ou software
  - Atacante interno
  - Roubo de equipamento
  - Atacante externo
  - Desastre natural
  - Espionagem industrial
  - Terrorismo

- **Alvos de ameaça**
  - A tabela abaixo lista alvos comuns:

Domínio	**Alvo de ameaça**
Domínio de usuário	PCs, smartphones, software e aplicativos.
Domínio de estação de trabalho	Estações de trabalho administrativas, estações de trabalho e servidores departamentais, software de rede e de sistemas operacional
Domínio de LAN	Servidores de arquivos, servidores de impressão/e-mail/banco de dados/LAN, hubs, repetidores, switches.
Domínio de LAN para WAN	Servidores HTTP, servidores de e-mail/FTP, roteadores, firewall, hub, repetidores.
Domínio de WAN	Roteadores, pilhas e memórias temporárias (buffers) de TCP/IP, firewalls, gateways, switches.
Domínio de acesso remoto	VPNs, software de VPN.
Domínio de sistema/aplicativo	Sistemas operacionais de desktop/servidor de rede, aplicativos e servidores de e-mail, aplicativos e sistemas de planejamento de recursos empresárias (ERP), navegadores web.

Ataques maliciosos

- Um **ataque** em um sistema computacional ou em um ativo de rede obtém sucesso ao explorar uma vulnerabilidade do sistema.
- Existem quatro categorias gerais de ataque. Um ataque pode consistir em todas ou em uma combinação destas quatro categorias:
  - **Fabricações**: Envolve a criação de alguma fraude de modo a enganar usuário não suspeitos.
  - **Interceptações**: Uma interceptação envolve escutar transmissões e redirecioná-las para uso não autorizado.
  - **Interrupções**: Uma interrupção causa uma quebra em um canal de comunicação, o que bloqueia a transmissão de dados.
  - **Modificações**: Uma modificação é a alteração de dados contidos em transmissões ou arquivos.

Ataques maliciosos

- Ameaças de segurança podem ser ativas ou passivas:
  - Um **ataque ativo** envolve uma modificação do fluxo de dados ou tentativas de obter acesso não autorizado a sistemas de computação e de rede.
  - Em um **ataque passivo**, o atacante não faz mudanças no sistema. Esse tipo de ataque apenas intercepta e monitora transmissões.

Ataques maliciosos

- Ameaças ativas incluem:
  - Ataque de força bruta
  - Ataque de dicionário
  - Falsificação de endereço
  - Sequestro
  - Ataques de retransmissão
  - Ataques de homem no meio
  - Disfarce
  - Engenharia Social
  - Phishing
  - Phreaking
  - Pharming

Ataques maliciosos

- **Ataque de força bruta**
  - Atacante tenta diferentes senhas em um sistema até que uma delas tenha sucesso.
  - Normalmente é empregado um software que experimenta todas as combinações possíveis de uma provável senha, ID de usuário ou código de segurança, até que localize uma coincidência.
  - Esse tipo de ataque é chamado de ataque de força bruta porque o atacante simplesmente explora o código todo. Não existe habilidade ou furtividade envolvida: apenas força bruta que, por fim, quebra o código.

Ataques maliciosos

- **Ataque de dicionário**
  - É um ataque simples, que conta com senhas fracas escolhidas por usuários.
  - Um simples programa de invasão de senha pega todas as palavras de um arquivo de dicionário e tenta efetuar o acesso, inserindo cada verbete do dicionário como senha.

Ataques maliciosos

- **Falsificação de endereço (spoofing)**
  - Tipo de ataque em que uma pessoa, programa ou computador se disfarça, a fim de ganhar acesso a algum recurso.
  - Um ataque de falsificação comum envolve apresentar um endereço falso de rede para fingir ser um computador diferente.
  - Um ataque pode mudar o endereço de rede de um computador para se parecer com um computador autorizado na rede do alvo.

Ataques maliciosos

- **Sequestro (hijacking)**
  - Tipo de ataque em que o atacante toma o controle de uma sessão entre duas máquinas e se disfarça como uma delas. Existem alguns tipos de sequestro:
    - Sequestro de homem no meio - O atacante usa um programa para tomar o controle de uma conexão, disfarçando-se como cada ponta da conexão. Esse ataque permite que o atacante ganhe acesso às mensagens ou as modifique antes de retransmiti-las.
    - Sequestro de navegador - O usuário é direcionado a um web site diferente daquele que ele solicitou, normalmente para uma página falsa criada pelo atacante.
    - Sequestro de sessão - O atacante tenta assumir uma conexão existente entre dois computadores em rede.

Ataques maliciosos

- **Ataques de retransmissão (replay)**
  - Envolvem capturar pacotes de dados de uma rede e retransmiti-los para produzir um efeito não autorizado.
  - O recebimento de pacotes IP duplicados e autenticados pode perturbar um serviço ou ter outra consequência indesejada.
  - Sistemas podem ser interrompidos por meio de ataques de retransmissão quando atacantes reutilizam mensagens antigas ou partes delas para enganar usuários de um sistema. Isso ajuda intrusos a obter informações que permitam acesso não autorizado a um sistema.

Ataques maliciosos

- **Ataque de homem no meio (man in the middle)**
  - Atacante intercepta mensagens entre duas partes antes de transferi-las para seu destino pretendido.
  - Falsificação na web é um tipo de ataque man in the middle no qual o usuário acredita que existe uma sessão segura com um servidor web específico. Na realidade, a conexão segura só existe com o atacante e não com o servidor web. O atacante, então, estabelece uma conexão segura com o servidor web e passa o tráfego entre o usuário e o servidor. Desse modo, o atacante pode enganar o usuário para fornecer senhas, informações de cartão de crédito e outros dados privativos.

Ataques maliciosos

- **Ataque de disfarce (masquerade attack)**
  - Um usuário ou computador finge ser outro.
  - Normalmente incluem uma das outras formas de ataques ativos, como falsificação de endereço ou retransmissão.
  - Atacantes podem capturar sequências de autenticação e depois reproduzi-las mais tarde, para acessar novamente um aplicativo ou sistema operacional.

Ataques maliciosos

- **Engenharia Social**
  - Envolver enganar usuários autorizados para que executem ações para usuários não autorizados.
  - Seu sucesso depende da tendência básica das pessoas em querer ser útil.
  - Coloca o elemento humano no circuito de brechas de segurança e o utiliza como arma. Uma identidade de vendedor ou funcionário forjada ou roubada pode oferecer entrada para um local seguro. O intruso pode então obter acesso a ativos importantes.

Ataques maliciosos

- Algumas técnicas para reduzir o impacto da engenharia social:
  - Treinamento para funcionários nos fundamentos de um ambiente seguro.
  - Política de segurança e de uso de computadores.
  - Política rígida para procedimentos de suporte técnico interno e externo.
  - Exigência do uso de identificações.
  - Limitação dos dados acessíveis ao público.
  - Cuidado ao usar acesso remoto.
  - Ensino de técnicas para enviar e receber mensagens seguras de e-mail.

Ataques maliciosos

- **Preaking**
  - É uma gíria que descreve a atividade de uma subcultura de pessoas que estudam, experimentam ou exploram sistemas telefônicos, equipamento de companhia telefônica e sistemas conectados a redes públicas de telefone.
  - Preaking de telefone é a arte de explorar erros e defeitos do sistema telefônico.

Ataques maliciosos

- **Phishing (roubo de identidade)**
  - Tipo de fraude em que um atacante tenta enganar a vítima para obter informações privativas, como números de cartão de crédito, senhas, datas de nascimento, números de conta bancárias e outros.
  - Uma fraude de phishing é uma tentativa de cometer roubo de identidade por e-mail ou mensagem instantânea. A mensagem parece vir de uma fonte legítima e inclui uma solicitação urgente de informações pessoais.
  - A mensagem instrui a vítima a fornecer a informação solicitada ou clicar em um link fornecido. Clicar no link levará a vítima a um web site falso, que parece idêntico ao oficial, mas pertence ao golpista.

Ataques maliciosos

- Como identificar uma fraude de phishing
  - Phishers utilizam caracteres de aparência semelhante no lugar no caracteres reais em URL. Exemplo: caractere 1 no lugar da letra L minúscula.
  - Alguns links parecem legítimos, incluindo o certificado de segurança. Antes de clicar você deverá visualizá-lo para saber onde o levará.
  - Alguns phishers compram nomes de domínio semelhantes aos de empresas legítimas.
  - Um truque é usar o mesmo nome de domínio, mas com .org em vez de .com.

Ataques maliciosos

- **Pharming**
  - Outro tipo de ataque que busca obter informações financeiras pessoais ou privativas por meio de falsificação de domínio.
  - Um ataque de pharming não usa mensagens para enganar vítimas. Em vez disso, usa falsificação de domínio, "corrompendo" um servidor de sistemas de nomes de domínio (DNS).
  - O resultado é que, quando um usuário informa o endereço web do servidor corrompido em sua barra de endereço, ele navega até o site do atacante.

Software Maliciosos

- Alguns tipos de software se infiltram em um ou mais computadores-alvo e seguem instruções de um atacante, que podem incluir causar danos, escalar privilégios de segurança, divulgar dados privativos ou até mesmo modificar ou excluir dados. Este tipo de software é o **software malicioso** ou **malware**.
- A finalidade do malware é danificar ou corromper um sistema. Os efeitos podem varias desde tornar um PC lento, fazer com que falhe, até o roubo de informações sigilosas.

Software Maliciosos

- Malware existe em duas categorias principais de programas de infecção e programas de ocultação.
  - Programas de infecção tentam ativamente copiar a si mesmos para outros computadores. Sua funcionalidade principal é executar instruções de um atacante em novos alvos. Malware desse tipo inclui:
    - Vírus
    - Vermes (*Worms*)
  - Programas de ocultação se escondem no computador, executando as instruções do atacante enquanto evitam a detecção. Os malwares que se ocultam incluem:
    - Cavalos de tróia (*Trojan*)
    - Rootkits
    - Programas espiões (*Spywares*)

- **Vírus**
  - Vírus é um software que se conecta a outro ou se copia para outro programa em um computador.
  - Sua finalidade é enganar o computador para seguir instruções não intencionadas pelo desenvolvedor original do programa.
  - Usuários copiam arquivos infectados de outro computador em uma rede, a partir de um pen-drive ou de um serviço on-line.

Software Maliciosos

- O 1º vírus registrado foi o Creeper, escrito pelo pesquisador Bob Thomas, em 1971. Creeper se copiava para outros computadores em rede, exibindo a mensagem "I'm the creeper, catch me if you can!".
- Hoje, milhares de vírus conhecidos infectam programas de todos os tipos. Quando um usuário executa programas infectados, na realidade estão executando código de vírus com suas credenciais de usuário e autorização. O vírus não precisa escalar privilégios; o usuário que executa o programa infectado fornece ao vírus suas próprias credenciais e permissões autenticadas.

- **Vermes (Worms)**
  - Programa autocontido que se replica e envia cópias de si mesmo para outros computadores, geralmente por uma rede.
  - Sua finalidade pode ser reduzir disponibilidade, usando a largura de banda da rede, ou tomar outras ações indevidas.
  - A principal diferença entre um vírus e um worm é que este não precisa de um programa hospedeiro para infectar. Trata-se de um programa isolado.

Software Maliciosos

- O primeiro worm relatado a se espalhar "em campo" foi o Morris, escrito por Robert Tappan Morris em 1988.
  - O worm atacou uma vulnerabilidade de estouro de buffer.
  - A intenção inicial era estimar o tamanho da internet, espalhando-se e infectando versões do sistema operacional UNIX. Porém, o worm se espalhou mais rapidamente do que o autor esperava. Por fim, infectou computadores várias vezes, tornando finalmente mais lento cada computador infectado, até o ponto em que se tornava inutilizável.
  - O Morris foi o primeiro incidente de malware a receber atenção geral da mídia e resultou na primeira condenação sob lei de uso e fraude de computadores de 1986 nos EUA.

- **Cavalos de Tróia (Trojan)**
  - Malware que se disfarça como um programa útil.
  - Se parecem com programas que realizam tarefas úteis, mas, na verdade, ocultam um malicioso código. Uma vez que o programa é executado, as instruções de ataque são executadas com as permissões e a autoridade do usuário.
  - Uma vez que o programa é executado, as instruções de ataque são executas com as permissões e a autoridade do usuário.

Software Maliciosos

- O primeiro trojan conhecido foi o Animal, lançado em 1974.
  - Animal se disfarçava como um jogo simples de charadas, no qual o usuário pensava em um animal e o programa fazia perguntas para tentar adivinhá-lo. Porém, além de fazer perguntas, o programa se copiava em cada diretório ao qual o usuário tinha acesso para gravação.
- Os trojans de hoje fazem muito mais que salvar cópias de si. Eles podem ocultar programas que coletam informações confidenciais, abrem portas do fundos em computadores ou carregam e baixam arquivos ativamente.

- **Rootkit**
  - Rootkits são mais novos que os outros tipos de malware, apareceram no início da década de 90.
  - É um tipo de malware que modifica ou substitui um ou mais programas existentes para ocultar vestígios de ataque.
  - Embora normalmente modifiquem partes do sistema operacional para esconder vestígios de sua presença, eles podem existir em qualquer nível - desde instruções de partida (boot) de um computador até aplicativos que são executados no sistema operacional.
  - Uma vez instalados, rootkits fornecem a atacantes acesso fácil para computadores comprometidos lançarem ataques adicionais.

Software Maliciosos

- Rootkits existem para diversos sistemas operacionais, incluindo Linux, Unix e Microsoft Windows.
- Uma vez instalados podem ser difíceis de detectar e remover. Porém, um IDS baseado em servidor pode ajudar a detectar atividades de rootkits.
- Se detectado, uma solução é restaurar o sistema operacional a um ponto seguro. Impedir acesso não autorizado, que possa permitir a um atacante instalar um rootkit é muito mais efetivo que tentar remover um rootkit instalado.

- **Programa Espião (Spyware)**
  - Tipo de malware que ameaça especificamente a confidencialidade de informação.
  - Ele colhe informações sobre um usuário por meio de uma conexão de Internet sem seu conhecimento.
  - Um spyware às vezes é agrupado como um componente de programas *freeware* ou *shareware* que usuários baixam da Internet.
  - Uma vez instalado, ele monitora as atividade de um usuário na Internet e pode colher informações como endereços de e-mail e até mesmo senhas e números de cartão de crédito.

Software Maliciosos

- Como um programa espião existe como programa executável independente, ele pode realizar uma série de operações, incluindo:
  - Monitorar toques de teclas;
  - Varrer arquivos no disco rígido;
  - Bisbilhotar outros aplicativos, como programas de bate-papo ou processadores de texto;
  - Instalar outros programas espiões;
  - Ler cookies;
  - Alterar a página inicial padrão do navegado web.

Combatendo Malware

- É sempre melhor evitar malware que ter reparar dandos causados por ele. A seguir, seis etapas gerais para impedir malwares.
  1. Crie um programa educacional para os usuários;
  2. Poste boletins regulares sobre problemas de malware;
  3. Nunca transfira arquivos de uma fonte desconhecida ou não confiável, a menor que o computador tenha um utilitário antimalware instalado;
  4. Teste novos programas ou abra arquivos suspeitos em máquinas virtuais;
  5. Instale software antimalware, certifique-se de sua atualização;
  6. Use um processo seguro de controle de acesso e autenticação;

Combatendo Malware

- Outra tática importante para combater malware é manter-se em dia com desenvolvimentos de malware.
- Acompanhe informativos mais recentes sobre o assunto.
- Sites com informações sobre malware:
  - *National Cyber Security Alliance* - NCSA - www.staysafeonline.org
  - *Computer Security Institute* - CSI - www.csisite.net
  - *United Satates Computer Emergency Readiness Team* - US-CERT - www.us-cert.gov

Combatendo Malware

- Além disso, você deverá usar software antimalware em seu sistema para varrer todos os arquivos introduzidos em estações de trabalho.
- Existem muitos produtos, entre eles:
  - Bitdefender
  - Kaspersky Anti-Vírus
  - Norton Antivirus
  - ESET Nod32 Antvírus
  - AVG Anti-Vírus
  - Avira AntiVir
  - Trend Micro
  - Microsoft Security Essentials

Referências

- Fundamentos de Segurança de Sistemas de Informação - David Kim; Michael G. Solomon