
CYBER
ACADEMY
FEBRABAN

MÓDULO 4

# Ameaças Cibernéticas

**Conceito**
O termo Ameaça Cibernética se refere a situações, mecanismos e ações maliciosas realizadas por pessoas mal-intencionadas em busca de explorar vulnerabilidades de rede, sistemas e dispositivos tecnológicos. Os atores maliciosos para praticar suas ações, utilizam-se de diversos mecanismos para conseguir alcançar o seu objetivo de comprometer algum sistema ou dispositivo tecnológico.

Vamos falar um pouco de algumas ameaças conhecidas, explicar o que elas são e quais impactos elas podem gerar a uma companhia ou pessoa diretamente.

**Virus de Boot**

**O que é:**
Trata-se de um tipo de malware que infecta o setor de inicialização de um disco rígido ou de dispositivos de armazenamento. Na fase inicial, ele se espalha pelo dispositivo infectado, como, por exemplo, um pen drive USB. Se esse dispositivo estiver conectado ao computador no momento do boot, o código malicioso é carregado diretamente na memória antes do Sistema Operacional.

**Como funciona:**
Esse malware é capaz de alterar e substituir o código legítimo do setor de inicialização. Dessa forma, sempre que o sistema for reiniciado, o malware será executado novamente.

**Como se propaga:**
Uma vez que o sistema é comprometido, o vírus tenta infectar outros dispositivos conectados, como unidades USB ou outros discos rígidos. Ele utiliza qualquer novo dispositivo para se propagar e comprometer outros sistemas.

**Impacto:**
O vírus pode causar desde problemas leves, como uma inicialização lenta, até consequências mais graves, como corrupção de dados, falhas no sistema ou até a incapacidade de iniciar o sistema.

**Como prevenir:**

- Uso de software antivírus: Utilize um software antivírus confiável para ajudar na detecção e remoção de vírus de boot, protegendo o sistema desde o momento da inicialização.
- Configuração de boot seguro: As versões mais recentes de sistemas operacionais, como Windows 10 e 11, vêm com a função UEFI (Unified Extensible Firmware Interface), que ativa o Secure Boot, substituindo o BIOS tradicional e oferecendo uma camada extra de segurança durante o processo de inicialização.

**Virus Time Bomb**

**O que é:**
É um malware projetado para permanecer inativo dentro de um sistema até que haja uma condição especifica a ser atendia, pode ser uma data ou hora. Assim que essa condição for alcançada o vírus é ativado e a sua carga maliciosa e o executa.
Ele é ativado especificamente com base do tempo, ou seja, o gatilho aciona o código maliciosos e um evento temporal com data e hora específica.

**Como funciona:**
Ele pode se infiltrar no sistema de diversas maneiras, como por meio de downloads, e-mails com anexos infectados, ou explorando vulnerabilidades de softwares. Após infectar o alvo, ele permanece inativo e indetectável.

**Como se propaga:**
Como ele é programado para “explodir” ou ativar em uma situação específica, quando esse gatilho é acionado, o vírus executa sua carga, que pode variar desde a exibição de mensagens inofensivas até a exclusão de arquivos, corrupção de dados ou até mesmo a formatação de um disco rígido.

**Impacto:**
Esse vírus pode ocasionar danos significativos de acordo com o proposito em que ele foi programado para fazer.

**Como prevenir:**

- Software antivírus atualizado: Mantenha o software antivírus sempre na última versão recomendada pelo fornecedor, garantindo também que a base de dados de ameaças esteja constantemente atualizada.
- Atualização de Sistema Operacional e softwares: Para evitar que vulnerabilidades

conhecidas sejam exploradas, mantenha o sistema operacional e os softwares sempre atualizados, aplicando todos os patches de segurança disponíveis.
• Realização de backups regulares: Estabeleça rotinas de backup frequentes para proteger seus dados, garantindo que, em caso de infecção por malwares como o Time Bomb, você possa recuperar informações sem perdas significativas.

**Worm**

**O que é:**
É um tipo de malware que se propaga automaticamente, replicando-se de um computador para outro sem necessidade de intervenção humana para ativação. Ao contrário de outros vírus, que utilizam arquivos ou programas hospedeiros, o worm se espalha diretamente pelas redes de sistemas.

**Como funciona:**
Ele geralmente se infiltra em um sistema por meio de vulnerabilidades em software, anexos de e-mails maliciosos, downloads de arquivos infectados ou explorando falhas de segurança em sistemas operacionais, aplicativos ou redes.

**Como se propaga:**
Uma vez dentro de um sistema, o worm começa a se replicar automaticamente e tenta se espalhar para outros computadores na mesma rede ou através da internet. Ele envia cópias de si mesmo para todos os contatos do usuário, infecta dispositivos conectados e explora vulnerabilidades em redes e servidores.

**Impacto:**
Worms representam uma ameaça significativa às redes e sistemas, causando diversos problemas críticos. Ao se replicar e tentar se espalhar para outros sistemas, eles podem gerar um tráfego massivo que congestiona a rede, resultando em lentidão ou até mesmo na interrupção do serviço. Além disso, o alto volume de solicitações geradas por esses worms pode sobrecarregar servidores, levando à sua indisponibilidade. Alguns worms instalam backdoors nos sistemas infectados, permitindo que atacantes obtenham acesso remoto para controlar os sistemas, roubar dados ou lançar ataques subsequentes. Além disso, esses worms podem carregar outros malwares, como ransomware, keyloggers e trojans, ampliando ainda mais o impacto negativo sobre os alvos.

**Versões conhecidas:**
• Morris Worm (1988): Foi um dos primeiros worms amplamente conhecidos causou grandes interrupções na internet ao sobrecarregar sistemas com sua replicação.
• ILOVEYOU (2000): Esse worm se espalhou via e-mail com assunto “ILOVEYOU”, infectando milhões de computadores em todo mundo;

• SQL Slammer (2003): Esse worm se espalhou rapidamente, causando interrupções significativas em serviços bancários e aéreos, além de derrubar a rede de emergência 911 em Seattle.
• WannaCry (2017): Ele incorporou elementos de worm para explorar a vulnerabilidade no protocolo SMB do Windows, permitindo sua replicação e criptografia dos dados, com um pedido de resgate para fornecer a chave de acesso. Assim surgiu o conhecido e temido ransomware. Infectou em torno de 230.000 computadores em 150 países e gerou prejuízos de bilhões segundo a CNN na época.

**Como prevenir:**

• Software antivírus atualizado: Garanta que o software antivírus esteja sempre na versão mais recente recomendada pelo fornecedor, incluindo a atualização constante de sua base de dados, para detectar e neutralizar ameaças de maneira eficaz.
• Manter Sistema Operacional e softwares atualizados: Aplique as atualizações e patches de segurança regularmente em sistemas operacionais e softwares, prevenindo que vulnerabilidades conhecidas sejam exploradas por malwares.
• Configurar Firewall: Configure firewalls para monitorar e controlar o tráfego de rede, bloqueando portas e protocolos desnecessários, o que ajuda a evitar a propagação de worms dentro da rede.
• Segurança de Rede: Separe redes internas de redes externas e limite o compartilhamento de arquivos. Além disso, utilize senhas fortes e implemente a autenticação multifator (MFA) para proteger acessos a sistemas e dispositivos.
• Backup Regular: Realize backups regulares dos dados, possibilitando a restauração dos sistemas sem perdas significativas em caso de infecção.
• Educação e Conscientização: Promova treinamentos internos para que os usuários possam identificar e-mails de phishing, links suspeitos e downloads de fontes não confiáveis, prevenindo métodos comuns de disseminação de worms.

**Botnets**

**O que é:**
São redes de computadores infectados controlados remotamente por um atacante, conhecido com bootmaster. OS computadores infectados podem ser chamados de bots ou zumbis, são usados de formas coordenadas para realizar atividades maliciosas.

**Como funciona:**
Ele possui 2 fases de execução:

1- Infecção: O computador é infectado por um malware que transforma em um bor. Isso ocorre através de downloads maliciosos, e-mails phishing ou exploração de vulnerabilidades no sistema.

2- Controle Remoto: O bootmaster controla o botnet remotamente, por meio de servidores de comando e controle (C&C). Enviando comandos aos bots para executar atividades maliciosas, como ataques DDos, envio de spam, roubo de dados, mineração de criptomoedas.

**Como se propaga:**
Uma vez que o computador está em controle do bootmaster , ele pode tentar infectar outros sistemas, aumentando o tamanho do botnet e consequentemente o poder de ataque na rede.

**Impacto:**
Elas frequentemente lançam ataques de DDoS, onde um grande número de bots sobrecarrega servidores ou redes com tráfego excessivo, tornando-os inacessíveis aos usuários legítimos. Além disso, botnets são usadas para enviar milhões de e-mails de spam e phishing, que contêm links ou anexos maliciosos, capazes de infectar computadores ou roubar informações pessoais e financeiras. Outra utilização comum é na mineração de criptomoedas, como Bitcoin e Monero, onde os botmasters aproveitam o poder de processamento dos computadores infectados, resultando em lentidão significativa dos sistemas e aumento nos custos de energia.

**Como prevenir:**

- Software antivírus atualizado: Mantenha o software antivírus sempre na versão mais recente recomendada pelo fornecedor, garantindo que a base de dados de ameaças esteja constantemente atualizada.
- Atualização de Sistemas Operacionais e softwares: Para prevenir a exploração de vulnerabilidades, mantenha o sistema operacional e os softwares sempre atualizados, aplicando todos os patches de segurança disponíveis.
- Configuração de Firewall e Segurança de Rede: Utilize firewalls para monitorar e controlar o tráfego de rede, bloqueando portas e protocolos suspeitos que possam ser usados por botnets para comunicação. Além disso, monitore a rede regularmente para detectar atividades anômalas.
- Utilização de Autenticação Multifator (MFA): Implemente MFA como uma camada extra de segurança para contas e sistemas da empresa. Mesmo que um botnet capture as credenciais, o MFA impede o acesso não autorizado.
- Educação e Conscientização: Promova treinamentos internos para que os usuários aprendam a identificar e-mails de phishing, links suspeitos e downloads de fontes não confiáveis, além de práticas seguras de navegação na internet, reduzindo assim o risco de infecções.

**Deface**

**O que é:**
É um tipo de ataque cibernético em que um invasor altera o conteúdo visual de um

site ou página web, substituindo-o por ias próprias mensagens, imagens ou vídeos. Esse tipo de ataque é frequentemente usado para propaganda políticas, mensagens hacktivistas, ou simplesmente para demonstrar suas habilidades em comprometer um site. O objetivo é principal do deface é geralmente para prejudicar a reputação da organização alvo.

**Como funciona:**
Os ataques a servidores web frequentemente começam com a exploração de vulnerabilidades em sistemas, como em software de gerenciamento de conteúdo (CMS) ou em plugins instalados. As vulnerabilidades mais comuns incluem XSS, SQL injection e credenciais fracas, que podem ser exploradas através de ataques de força bruta. Uma vez que a vulnerabilidade é explorada, o invasor ganha acesso ao back end do site ou servidor web, permitindo a modificação de arquivos críticos, páginas HTML, arquivos CSS e scripts. Com esse acesso, o atacante pode alterar o conteúdo do site, substituindo-o por suas próprias mensagens, que podem incluir texto, imagens, vídeos ou links maliciosos. Esse tipo de ataque é frequentemente associado ao hacktivismo e pode conter conteúdo político ou ofensivo. Embora o deface em si não se propague como um worm ou vírus, se o invasor tiver acesso a múltiplos sites ou servidores, como em ambientes de hospedagem compartilhada, ele pode realizar ataques de deface em várias páginas simultaneamente.

**Como se propaga:**
O deface não se propaga como um worm ou vírus. No entanto, se o invasor tiver acesso a múltiplos sites ou servidores (exemplo: hospedagem compartilhada) ele pode realizar o deface em várias páginas ao mesmo tempo.

**Impacto:**
Dados à reputação e Perda de Receita: O impacto imediato de um deface é o dano à reputação da organização, onde visitantes perdem a confiança na empresa acreditando que ela não possui práticas de segurança.  Logo, isso afeta a parte monetária perdendo receita devido a exposição sofrida, principalmente se for uma empresa de e-commerce.

**Como prevenir:**

- Manter Softwares e CMS Atualizados: Assegure que o sistema operacional do servidor, o CMS e todos os plugins estejam sempre atualizados com os patches de segurança fornecidos pelos fornecedores, minimizando vulnerabilidades.
- Uso de Senhas Fortes e Autenticação Multifator (MFA): Utilize senhas complexas e implemente a autenticação multifator (MFA) para todos os usuários com acesso ao backend do site, reforçando a segurança das contas e prevenindo acessos não autorizados.
- Configuração Segura do Servidor Web: Configure o servidor web seguindo as melhores práticas de segurança, como desativar scripts e serviços desnecessários, ajustar permissões de arquivos e diretórios com base no Controle de Acesso Baseado em Função (RBAC) e adotar frameworks de boas práticas como o OWASP.

• Educação e Conscientização: Treine sua equipe para reconhecer e responder rapidamente a sinais de comprometimento de segurança. Incentive-os a evitar clicar em links suspeitos, usar redes seguras e relatar qualquer atividade anômala.
• Backup Regular do Site: Realize backups regulares do conteúdo do site e armazene-os em locais seguros, fora do alcance de atacantes, garantindo a integridade dos dados e a capacidade de recuperação.
• Implementação de WAF (Web Application Firewall): Utilize um WAF para bloquear ataques comuns e conhecidos, como SQL injection e XSS, fortalecendo a proteção do seu site contra ameaças e mantendo a segurança dos dados.

**Cavalo de Troia**

**O que é:**
É um malware disfarçado de software legitimo que, uma vez executado realizada atividades maliciosas no sistema da vítima. Como roubo de dados, controle remoto, instalações de outros malwares dentre diversos outros cenários.

**Como funciona:**
O trojan geralmente se apresenta como um arquivo ou programa legitimo, como por exemplo um anexo de e-mail, jogos ou até mesmo uma atualização de software em um site que não seja do vendor. Quando usuário executa o trojan ele instala o malware no sistema sem que seja perceptível ao usuário e começa a correr em segundo plano.
Ao realizar esse processo começa a executar a sua função, no caso a ação maliciosa que ele foi programado. Roubar dados, instalar outros malwares, controle remore entre outras atividades.

**Como se propaga:**
Ele pode se propagar através de downloads de softwares falsos, e-mail de phishing com anexos maliciosos, sites comprometidos e dispositivos de armazenamento.

**Impacto:**
Um dos principais objetivos é o roubo de informações pessoais e financeiras, como logins, dados de cartões de crédito e informações sensíveis. Além disso, os atacantes podem obter controle remoto sobre sistemas infectados, realizando atividades como espionagem, instalação de malwares adicionais e utilização dos sistemas comprometidos para atacar outras redes. Isso também compromete os recursos do sistema afetado, causando lentidão significativa devido ao uso excessivo de CPU e memória. Outro efeito devastador é a perda e corrupção de dados, com arquivos sendo apagados, corrompidos ou criptografados, resultando na perda de dados valiosos. Além disso, a desativação de programas de segurança e firewalls torna o sistema ainda mais vulnerável a futuros ataques.

**Versões Conhecidas:**

- Trojan Destrutivo: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
- Trojan Spy: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
- Trojan Banker ou Bancos: coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy, porém com objetivos mais específicos.

**Como prevenir:**

- Software antivírus atualizado: Mantenha o software antivírus sempre na versão mais recente recomendada pelo fornecedor, e assegure-se de que a base de dados de ameaças esteja constantemente atualizada para garantir a detecção eficaz de novas ameaças.
- Atualização de Sistemas Operacionais e softwares: Para prevenir a exploração de vulnerabilidades, mantenha o sistema operacional e todos os softwares atualizados com os patches de segurança mais recentes.
- Uso de Senhas Fortes e Autenticação Multifator (MFA): Utilize senhas complexas e ative a autenticação multifator (MFA) para todos os usuários com acesso ao sistema, adicionando uma camada extra de proteção.
- Evitar downloads de sites não confiáveis e cuidado com e-mails suspeitos: Evite baixar softwares de fontes não confiáveis e não clique em links ou baixe anexos de e-mails de remetentes desconhecidos. Caso identifique atividades suspeitas, reporte imediatamente à equipe de segurança.
- Educação e Conscientização: Instrua os usuários a reconhecer sinais de phishing e práticas de engenharia social, promovendo a identificação e o reporte rápido de possíveis ameaças à equipe de segurança.

**Keylogger**

**O que é:**
É um tipo de software ou hardware projetado para registrar teclas pressionadas em um teclado, geralmente sem o conhecimento ou consentimento do usuário. O objetivo principal do keylogger é capturar informações, sendo elas sensíveis ou não.

**Como funciona:**
Ele monitora e registra cada tecla pressionada no teclado. Ele pode capturar tudo o que é digitado, incluindo senhas, mensagens de texto etc. Qualquer imput de texto ele irá registrar. Ele tem a capacidade de armazenar ou transmitir os dados remotamente via internet, alguns mais sofisticados tampem podem capturar a tela, registrar cliques do mouse até gravar atividades de clipboard. Ele possui a habilidade de operar de forma oculta sem dar sinais de sua presenta, podendo ser integrados a outros malwares como

trojans embutimos em aplicativos aparentemente inofensivos.

**Keyloggers Baseados em Softwares:**

- Keyloggers de API: Usam APIs do sistema operacional para capturar eventos de teclas.
- Keyloggers de Formulário: Interceptam dados digitados em formulários da web.
- Keyloggers de Kernel: Funcionam em um nível mais profundo do sistema operacional, capturando as teclas antes que cheguem ao aplicativo.

**Keyloggers Baseados em Hardware:**

- Dispositivos de Hardware: Pequenos dispositivos físicos conectados entre o teclado e o computador, que capturam as teclas pressionadas.
- Keyloggers de Firmware: Instalados diretamente no firmware do teclado, interceptando as teclas antes que elas sejam transmitidas ao computador.

**Como se propaga:**

Keyloggers de software são frequentemente distribuídos como parte de outros malwares, como Trojans, que podem ser instalados através de e-mails de phishing, downloads maliciosos, ou exploits de vulnerabilidades.

- Downloads Maliciosos: Eles podem ser disfarçados como softwares legítimos ou incluídos em pacotes de instalação de software de fontes não confiáveis.

- Acessórios de Hardware: Keyloggers de hardware podem ser fisicamente conectados ao computador, geralmente por alguém com acesso físico aos dispositivos.

**Impacto:**

Keyloggers representam uma ameaça significativa à privacidade do usuário, ao registrar conversas privadas, e-mails e outras comunicações sensíveis. As informações capturadas podem ser utilizadas para cometer fraudes financeiras, roubo de identidade e outros crimes cibernéticos. Além disso, empresas afetadas por keyloggers podem sofrer danos reputacionais severos, perda de confiança dos clientes e enfrentar possíveis ações legais, agravando ainda mais as consequências de um compromisso de segurança.

**Como prevenir:**

- Software antivírus atualizado: Mantenha o software antivírus sempre na versão mais recente recomendada pelo fornecedor, garantindo que inclua mecanismos eficazes para a detecção e remoção de keyloggers, além de manter a base de dados de ameaças atualizada.
- Atualização de Sistema Operacional e softwares: Para evitar a exploração de vulnerabilidades, mantenha o sistema operacional e todos os softwares sempre atualizados com os patches de segurança mais recentes.
- Uso de Autenticação Multifator (MFA): Mesmo que um keylogger capture uma

senha, a autenticação multifator (MFA) pode prevenir o acesso não autorizado ao exigir uma segunda forma de verificação.
• Evitar downloads de sites não confiáveis e cuidado com e-mails suspeitos: Evite baixar softwares de fontes não confiáveis e não clique em links ou baixe anexos de e-mails de remetentes desconhecidos. Caso identifique algo fora do comum, reporte imediatamente à equipe de segurança.
• Educação e Conscientização: Instrua os usuários a evitar clicar em links suspeitos, a não fazer downloads de fontes não confiáveis e a ser cautelosos ao abrir anexos de e-mails, promovendo práticas seguras de navegação.
• Teclados Virtuais e Gerenciadores de Senhas: Utilize teclados virtuais ou gerenciadores de senhas para reduzir a exposição a keyloggers, pois esses métodos evitam a captura das teclas reais pressionadas.

**Hijacker**

**O que é:**
É um tipo de malware que compromete o navegador, alterando suas configurações e redirecionando o tráfego do usuário para sites maliciosos ou cheios de anúncios. Ele pode se espalhar através de downloads de software gratuito, sites comprometidos, e-mails, ou extensões de navegador. O impacto inclui perda de privacidade, diminuição do desempenho do sistema, e aumento do risco de infecção por outros malwares.

**Como funciona:**
Um hijacker de navegador pode modificar configurações importantes, como a página inicial, o motor de busca padrão, as novas guias e adicionar extensões ou barras de ferramentas indesejadas, tudo sem o consentimento do usuário e dificultando a reversão dessas mudanças. Após comprometer o navegador, o hijacker redireciona o tráfego do usuário para sites específicos, que podem ser maliciosos ou cheios de anúncios. Além disso, ele pode injetar anúncios ou conteúdo indesejado, como pop-ups, banners ou links em páginas legítimas. Alguns hijackers também coletam dados sobre os hábitos de navegação do usuário, incluindo termos de busca e sites visitados, podendo vender essas informações a terceiros ou usá-las para outras atividades maliciosas.

**Como se propaga:**
Hijackers são frequentemente distribuídos através de diversos métodos, incluindo downloads de software gratuito, onde são incorporados em pacotes de adware. Eles também podem ser disseminados quando o usuário visita sites comprometidos ou maliciosos e é induzido a clicar em pop-ups ou anúncios que iniciam o download. Além disso, alguns hijackers são enviados como anexos de e-mail em campanhas de phishing. Outra forma comum de distribuição é por meio de extensões e plugins para navegadores, que muitas vezes são disfarçados como ferramentas úteis para enganar os usuários.

**Impacto:**
Comprometem a privacidade do usuário ao coletar informações sobre histórico de navegação, termos de pesquisa e dados pessoais. Além disso, restaurar as configurações do navegador pode ser desafiador, especialmente se o hijacker modificar configurações do sistema ou adicionar arquivos que reinstalam o malware. Eles também sobrecarregam o navegador com anúncios e pop-ups, resultando em uma diminuição significativa no desempenho do sistema. Ademais, ao redirecionar o usuário para sites maliciosos, os hijackers aumentam o risco de infecção por outros tipos de malware, como trojans, keyloggers ou ransomware.

**Como prevenir:**

- Downloads Cuidadosos: Sempre baixe softwares de fontes confiáveis e esteja atento durante a instalação para desmarcar opções que permitam a instalação de software adicional indesejado.
- Manter Software Atualizado: Mantenha o navegador e o sistema operacional atualizados com as últimas correções de segurança para evitar a exploração de vulnerabilidades.
- Usar Software Antivírus e Antimalware: Use soluções de segurança confiáveis para detectar e remover hijackers. Realize varreduras regulares no sistema.
- Verificar Extensões e Plugins: Revise regularmente as extensões e plugins instalados no navegador, removendo qualquer coisa desconhecida ou suspeita.
- Desconfiança de Pop-ups e E-mails Suspeitos: Evite clicar em pop-ups ou em links de e-mails desconhecidos, especialmente se eles solicitarem a instalação de software ou plugins.

**Rootkit**

**O que é:**
É um tipo de malware sofisticado que proporciona ao atacante acesso privilegiado e oculto a um sistema, permitindo que ele controle o sistema sem ser detectado. Ele pode se propagar através de exploits, downloads maliciosos, phishing, e até ataques físicos. O impacto inclui controle total do sistema, roubo de informações, e comprometimento de segurança.

**Como funciona:**
Após infectar um sistema, obtém privilégios elevados, geralmente no nível de administrador, permitindo que ele controle funções críticas do sistema operacional. Sua capacidade de ocultação é extremamente perigosa, pois ele pode esconder arquivos, processos, chaves de registro e até conexões de rede, tornando-se invisível para o software antivírus e para o administrador. Com esse acesso privilegiado, o rootkit manipula o comportamento do sistema, interceptando chamadas e alterando funções do kernel para esconder sua presença e a de outros malwares. Além disso, muitos rootkits oferecem controle remoto ao atacante, permitindo a execução de comandos,

roubo de informações, instalação de mais malwares e até participação em ataques DDoS.

**Como se propaga:**
Exploram vulnerabilidades no sistema operacional ou em software para obter acesso inicial ao sistema, instalando-se em níveis profundos como o kernel ou a BIOS. Eles podem ser distribuídos como parte de outros malwares, como trojans, que os usuários inadvertidamente instalam ao baixar software de fontes não confiáveis. Além disso, campanhas de phishing podem enganar os usuários para que executem anexos maliciosos que instalam o rootkit. Em alguns casos, rootkits também podem ser instalados fisicamente em um sistema comprometido por meio de dispositivos USB ou outras mídias removíveis.

**Impacto:**
Rootkits oferecem controle total do sistema ao operar no nível do kernel, permitindo aos atacantes realizarem quase qualquer ação, desde o roubo de dados até a destruição de informações. Eles ocultam a presença de malwares e atividades maliciosas, permitindo que os atacantes operem sem serem detectados por longos períodos. Além disso, rootkits podem ser usados para roubar informações sensíveis, como credenciais de login, dados financeiros e outras informações pessoais. Sua presença compromete seriamente a segurança do sistema, pois pode desativar ou manipular software de segurança e firewalls. Devido à sua capacidade de ocultação e manipulação, rootkits são extremamente difíceis de detectar e remover, muitas vezes exigindo medidas drásticas como a reinstalação completa do sistema operacional.

**Como prevenir:**

- Manter o Sistema Atualizado: Instale regularmente patches de segurança e atualizações para o sistema operacional e todos os softwares, especialmente aqueles que operam em níveis baixos, como drivers e firmware.
- Usar Software de Segurança Avançado: Utilizar soluções de segurança que incluem proteção contra rootkits, como antivírus com capacidade de escanear o nível do kernel e sistemas de detecção de intrusões (IDS).
- Configurar o Sistema com Mínimos Privilégios: Restrinja privilégios de administrador e use contas de usuário padrão para tarefas diárias. Quanto menos privilégios um usuário tem, menos provável é que um rootkit consiga acesso privilegiado ao sistema.
- Cuidado com Downloads e E-mails: Evite baixar software de fontes não confiáveis e seja cauteloso com anexos de e-mails, especialmente aqueles de remetentes desconhecidos.
- Utilizar Boot Seguro (Secure Boot): Ative o Secure Boot no BIOS/UEFI para garantir que apenas sistemas operacionais e drivers assinados sejam carregados durante a inicialização.

**Sniffer**

**O que é:**
É um software ou hardware usado para capturar e analisar o tráfego de rede. Ele funciona interceptando pacotes de dados e analisando seu conteúdo. Sniffers podem ser usados de forma maliciosa para roubar informações sensíveis e comprometer a privacidade. Eles podem se propagar através de instalação direta, ataques MitM, ou acesso físico.

**Como funciona:**
Um sniffer de rede intercepta pacotes de dados transmitidos através da rede, podendo capturar todos os pacotes ou apenas aqueles que atendem a critérios específicos, como endereços IP, portas ou protocolos. Após a captura, o sniffer analisa o conteúdo dos pacotes, que pode incluir informações como endereços IP de origem e destino, portas de comunicação e o payload dos pacotes, que pode conter dados sensíveis como senhas, mensagens e informações pessoais. Para realizar essa captura, o sniffer opera em modo promíscuo, permitindo que ele leia todos os pacotes que passam pela interface de rede, e não apenas aqueles destinados ao seu próprio dispositivo.

**Como se propaga:**
Sniffers podem ser instalados de várias maneiras para interceptar e analisar o tráfego de rede. A instalação direta pode ocorrer através de downloads maliciosos ou ataques de phishing, permitindo que o sniffer capture tráfego de qualquer dispositivo na mesma rede local. Em ataques Man-in-the-Middle (MitM), o atacante se posiciona entre duas partes que se comunicam na rede, utilizando um sniffer para interceptar e analisar o tráfego, frequentemente empregando técnicas como ARP spoofing ou DNS spoofing. Além disso, sniffers podem ser fisicamente instalados em dispositivos de rede, como roteadores ou switches, por alguém com acesso físico ao hardware, aumentando ainda mais a capacidade de captura e monitoramento do tráfego de rede.

**Impacto:**
Sniffers têm a capacidade de capturar informações sensíveis, como credenciais de login, números de cartões de crédito e dados pessoais, comprometendo a segurança e a privacidade dos usuários. Eles permitem a interceptação de comunicações, que pode ser utilizada para espionagem ou para obter dados confidenciais. Além disso, se o tráfego interceptado for alterado, pode haver um comprometimento da integridade das comunicações, resultando em fraudes ou ataques direcionados. A dificuldade de detecção é uma preocupação adicional, já que sniffers podem operar de maneira discreta e em redes onde o tráfego não é monitorado ativamente, tornando sua identificação e remoção desafiadoras.

**Como prevenir:**

- Criptografia de Dados: Utilize criptografia para proteger dados em trânsito. Protocolos como HTTPS, TLS e VPNs garantem que as informações sejam

criptografadas e, portanto, muito mais difíceis de serem interceptadas e compreendidas por sniffers.
• Segmentação de Rede: Segmente redes e use VLANs para limitar a visibilidade do tráfego entre diferentes partes da rede. Isso ajuda a isolar áreas da rede onde informações sensíveis são transmitidas.
• Autenticação e Controle de Acesso: Use autenticação forte e controle de acesso para limitar quem pode conectar-se à rede e configurar dispositivos de rede. Isso reduz o risco de instalação não autorizada de sniffers.
• Segurança de Dispositivos: Proteja dispositivos de rede, como roteadores e switches, com senhas fortes e atualize o firmware regularmente para corrigir vulnerabilidades conhecidas.
• Educação e Conscientização: Eduque os usuários sobre práticas seguras, como evitar clicar em links suspeitos e baixar software de fontes não confiáveis, que podem comprometer a segurança da rede.

**Backdoor**

**O que é:**
É um malware que permite acesso não autorizado a um sistema, geralmente ocultando sua presença e permitindo controle remoto. Pode se propagar através de injeções de código, exploits, phishing e ataques de rede. O impacto inclui controle remoto, roubo de dados, e comprometimento da segurança

**Como funciona:**
Uma backdoor é projetada para fornecer acesso não autorizado a um sistema, contornando os métodos de autenticação normais, seja por meio de uma porta aberta ou uma falha de software explorada pelo atacante. Após a instalação, a backdoor pode se ocultar para evitar a detecção, desativando ou evitando que programas antivírus e outras ferramentas de segurança identifiquem sua presença. Muitas backdoors permitem o controle remoto do sistema pelo atacante, possibilitando a execução de comandos, o acesso a arquivos e a instalação de outros malwares. Além disso, elas podem ser configuradas para iniciar automaticamente com o sistema, garantindo que o atacante mantenha o acesso mesmo após reinicializações ou atualizações.

**Como se propaga:**
Backdoors podem ser instaladas por diversas técnicas, começando com a injeção de código malicioso, onde elas fazem parte de um malware maior, como um Trojan, que o usuário inadvertidamente instala ao baixar e executar software de fontes não confiáveis. Elas também aproveitam exploits de vulnerabilidades conhecidas no sistema operacional ou em aplicativos para instalar o malware sem o conhecimento do usuário. Phishing e engenharia social são outras estratégias usadas, em que os atacantes enganam o usuário para executar um arquivo malicioso que instala a backdoor. Além disso, em redes comprometidas, a backdoor pode ser instalada através de ataques que

exploram falhas em serviços de rede ou protocolos.

**Impacto:**
Um atacante pode obter controle remoto do sistema, permitindo espionagem das atividades do usuário, acesso a dados sensíveis e monitoramento de comunicações. A backdoor facilita o roubo de informações valiosas, incluindo dados pessoais, financeiros e confidenciais. Sua presença compromete seriamente a segurança do sistema, pois pode ser usada para instalar outros malwares ou participar de ataques coordenados. Além disso, as backdoors são projetadas para serem discretas e difíceis de detectar, tornando sua remoção um desafio que pode exigir ferramentas especializadas e, em alguns casos, a reinstalação completa do sistema operacional.

**Como prevenir:**

- Atualizações e Patches: Mantenha o sistema operacional e todos os softwares atualizados com os últimos patches de segurança para corrigir vulnerabilidades que poderiam ser exploradas para instalar uma backdoor.
- Antivírus e Antimalware: Use soluções de segurança confiáveis que ofereçam proteção em tempo real e realizem varreduras regulares para detectar e remover backdoors e outros malwares.
- Segurança da Rede: Implemente firewalls e sistemas de detecção de intrusões (IDS) para monitorar e bloquear tráfego suspeito que possa indicar a presença de uma backdoor.
- Controle de Acesso: Restrinja privilégios de administrador e use senhas fortes e únicas para minimizar o risco de acesso não autorizado ao sistema.
- Educação e Treinamento: Eduque os usuários sobre os riscos de phishing e outras técnicas de engenharia social, e incentive a prática de segurança segura ao baixar e instalar software.
- Segurança Física: Proteja fisicamente o acesso aos dispositivos e servidores para evitar que um atacante possa instalar um backdoor diretamente no hardware.

**Hoax**

**O que é:**
Um hoax é um engano ou desinformação que se espalha por e-mail, redes sociais e outros meios digitais, geralmente com o objetivo de causar pânico, enganar ou manipular. Eles funcionam criando falsas alegações e apelando para emoções, e se propagam rapidamente através de compartilhamentos. O impacto inclui pânico desnecessário, disseminação de informações falsas e possível comprometimento de segurança.

**Como funciona:**
Um hoax geralmente se baseia em alegações falsas ou exageradas que apelam para o medo, curiosidade ou senso de urgência do destinatário, como informações sobre

vírus fictícios, golpes ou ameaças iminentes. Essas mensagens são projetadas para se propagar viralmente, frequentemente incluindo apelos emocionais, instruções falsas ou pedidos para encaminhar a mensagem para amigos e familiares, o que aumenta sua disseminação. Além disso, os hoaxes frequentemente empregam técnicas de manipulação psicológica, criando um senso de urgência ou medo para incentivar as pessoas a agirem rapidamente sem verificar a veracidade das informações.

**Como se propaga:**
Frequentemente se espalham por diversos canais, começando com e-mails onde os destinatários são instruídos a compartilhar a mensagem, muitas vezes disfarçada de alertas de segurança ou mensagens importantes. Nas redes sociais, a natureza viral facilita a propagação rápida de informações falsas por meio de compartilhamentos e repostagens. Mensagens de texto e aplicativos de mensagens também são usados para disseminar hoaxes, solicitando que os destinatários encaminhem a mensagem para seus contatos. Além disso, alguns hoaxes são publicados em sites ou blogs, frequentemente disfarçados como notícias legítimas ou informações úteis, aumentando ainda mais a sua disseminação.

**Impacto:**
Hoaxes podem causar pânico e ansiedade desnecessários entre os destinatários ao apelar para medos comuns, como a ameaça de um vírus ou golpe, levando a uma propagação de informações falsas que desinforma o público e cria confusão sobre questões importantes ou ameaças reais. Além disso, a disseminação desses hoaxes pode sobrecarregar sistemas de suporte técnico e de segurança com consultas e pedidos de ajuda desnecessários. Em alguns casos, hoaxes incluem instruções para baixar software ou clicar em links maliciosos, o que pode comprometer a segurança do sistema e roubar informações pessoais.

**Como prevenir:**

- Verificação de Fontes: Sempre verifique a origem de uma mensagem ou notícia antes de acreditar ou compartilhar. Utilize fontes confiáveis e verifique se a informação foi confirmada por autoridades ou especialistas.
- Educação e Conscientização: Eduque-se e eduque os outros sobre os sinais comuns de hoaxes e desinformação. Incentive a prática de pensamento crítico e a checagem de fatos.
- Não Compartilhar Sem Verificação: Evite compartilhar mensagens alarmantes ou informações não verificadas, especialmente se forem solicitadas a serem encaminhadas a outros.
- Uso de Ferramentas de Verificação: Utilize ferramentas de verificação de fatos e serviços online que possam confirmar a veracidade de uma mensagem ou notícia.

**Phishing Scam**

**O que é:**
Um phishing scam é um ataque cibernético que visa enganar as vítimas para que divulguem informações pessoais e financeiras ao se disfarçar como uma comunicação legítima. Ele se propaga principalmente através de e-mails, mensagens de texto e sites falsos, e pode resultar em roubo de identidade, fraude financeira e comprometimento de contas.

**Como funciona:**
É um ataque que se apresenta como uma comunicação aparentemente legítima, como um e-mail, mensagem de texto ou site falso que imita uma empresa conhecida, banco ou serviço online. Ele geralmente solicita que o destinatário forneça informações pessoais ou clique em um link para verificar ou atualizar seus dados. Esse link pode levar a um site falso que parece autêntico, mas foi projetado para coletar dados de login e outras informações confidenciais. Para aumentar a eficácia, os ataques de phishing frequentemente criam um senso de urgência ou medo, como a ameaça de suspensão de conta ou problemas de segurança, pressionando a vítima a agir rapidamente sem pensar. Quando a vítima fornece suas informações no site falso ou responde ao e-mail, os dados são enviados diretamente para os atacantes, que podem usá-los para cometer fraudes ou acessar contas pessoais.

**Como se propaga:**
O phishing é amplamente disseminado por meio de várias plataformas, começando com e-mails que parecem vir de fontes confiáveis e frequentemente contêm links para sites falsos ou anexos maliciosos. Além dos e-mails, ataques de phishing podem ocorrer através de mensagens de texto (smishing) e aplicativos de mensagens, onde links ou instruções enganosas são fornecidos. Em redes sociais, criminosos criam perfis falsos ou enviam mensagens diretas para coletar informações dos usuários. Além disso, sites falsos que imitam páginas de login de instituições financeiras ou serviços online são frequentemente utilizados, levando os usuários desavisados a fornecerem suas informações pessoais por meio de links maliciosos.

**Impacto:**
Os dados obtidos através de phishing podem levar a sérios danos, incluindo o roubo de identidade, onde os atacantes utilizam as informações para realizar transações fraudulentas ou abrir contas em nome da vítima. Informações bancárias ou de cartões de crédito também podem ser usadas para efetuar compras não autorizadas ou transferências de dinheiro, comprometendo financeiramente a vítima. Além disso, o acesso a contas de e-mail ou redes sociais permite que os atacantes enviem mais phishing scams para os contatos da vítima ou coletem informações adicionais. Esses ataques não só causam prejuízos financeiros, mas também podem resultar em danos significativos à reputação da vítima, especialmente se informações sensíveis forem divulgadas ou utilizadas para enganar outras pessoas.

**Como prevenir:**
• Verificação de E-mails e Links: Verifique cuidadosamente o remetente de e-mails e o URL dos links antes de clicar. Desconfie de mensagens que solicitam informações pessoais ou financeiras.
• Autenticação de Dois Fatores (2FA): Habilite a autenticação de dois fatores em contas importantes para adicionar uma camada extra de segurança, o que dificulta o acesso não autorizado, mesmo que as credenciais sejam comprometidas.
• Educação e Conscientização: Eduque-se e eduque os outros sobre os sinais de phishing e as práticas seguras para evitar ser enganado por mensagens falsas.
• Não Compartilhar Informações Sensíveis: Nunca forneça informações pessoais, senhas ou detalhes financeiros em resposta a solicitações não solicitadas, especialmente se a comunicação não puder ser verificada como legítima.
• Relatar Phishing: Se você receber uma tentativa de phishing, denuncie o incidente à empresa ou instituição que está sendo falsamente representada e, se possível, a autoridades de cibersegurança.

**Ransomware**

**O que é:**
É um tipo de malware que criptografa arquivos em um sistema e exige um resgate para liberar o acesso a esses arquivos. Ele se propaga através de phishing, vulnerabilidades de softwares, downloads maliciosos e redes. O impacto inclui perda de dados, interrupção de operações, custos financeiros e danos à reputação

**Como funciona:**
Após infectar um sistema, o ransomware criptografa os arquivos da vítima utilizando algoritmos de criptografia robustos, tornando-os inacessíveis sem a chave de descriptografia, que é mantida pelo atacante. O ransomware geralmente exibe uma mensagem de resgate na tela do dispositivo, informando sobre o ataque e fornecendo instruções sobre como pagar o resgate para obter a chave de descriptografia. Essa mensagem pode incluir um prazo para o pagamento, com ameaças de excluir os arquivos ou aumentar o valor do resgate se o prazo não for cumprido. Após o pagamento, a vítima precisa se comunicar com o atacante para receber a chave de descriptografia necessária para desbloquear os arquivos, mas não há garantia de que o atacante cumprirá a promessa.

**Como se propaga:**
Ransomware frequentemente se propaga através de campanhas de phishing, onde os usuários são enganados a abrir anexos maliciosos ou clicar em links que baixam o malware. Além disso, exploits de vulnerabilidades em sistemas operacionais, aplicativos ou serviços de rede podem ser usados para distribuir ransomware, comprometendo redes inteiras por meio de falhas conhecidas. A infecção também pode ocorrer quando a vítima baixa e executa software de fontes não confiáveis ou comprometidas,

que contém o ransomware. Em redes locais e compartilhamentos de arquivos, o ransomware pode se espalhar, infectando outros dispositivos conectados. Ataques que utilizam senhas fracas ou comprometidas podem facilitar o acesso aos sistemas e permitir a instalação do ransomware.

**Impacto:**
A criptografia dos arquivos pelo ransomware impede que as vítimas acessem dados, resultando na perda de informações importantes, como documentos de negócios, arquivos pessoais e bancos de dados. Além disso, organizações e empresas podem enfrentar interrupções significativas em suas operações, com sistemas e serviços essenciais ficando fora de operação. Os custos financeiros são elevados, englobando não apenas o valor do resgate, mas também despesas com a recuperação de sistemas, perda de produtividade e possíveis multas regulatórias, sem garantia de que os arquivos serão efetivamente descriptografados. O impacto também se reflete na reputação, com empresas e instituições sofrendo danos, especialmente se a violação afetar clientes ou parceiros comerciais. Além disso, mesmo após o pagamento do resgate, não há garantia de que o ransomware não tenha sido projetado para infectar outros dispositivos ou se reinstalar.

**Como prevenir:**

- Backups Regulares: Realize backups regulares e mantenha cópias offline ou em locais de armazenamento separados. Isso garante que você possa restaurar dados sem pagar o resgate em caso de infecção.
- Atualização e Patch de Software: Mantenha todos os sistemas e softwares atualizados com os últimos patches de segurança para proteger contra vulnerabilidades conhecidas.
- Educação e Treinamento: Eduque usuários sobre os riscos de phishing e práticas seguras de navegação. Encoraje a verificação de e-mails e links antes de abrir anexos ou clicar em links.
- Controle de Acesso e Privilégios: Restrinja privilégios de usuário e controle o acesso a dados e sistemas críticos para minimizar o impacto de uma possível infecção.
- Políticas de Segurança: Desenvolva e implemente políticas de segurança robustas, incluindo planos de resposta a incidentes e procedimentos para lidar com ataques de ransomware.
- Desativar Macros: Desative macros em documentos recebidos por e-mail, pois muitas variantes de ransomware são distribuídas através de anexos de documentos com macros maliciosos.

À medida que as tecnologias avançam, novas ameaças surgem acompanhando esse progresso. Isso leva as organizações a investirem continuamente em segurança, mantendo o foco em três aspectos essenciais: pessoas, processos e tecnologias. Mesmo com investimentos significativos em ferramentas de segurança, a eficácia dessas soluções depende crucialmente do treinamento e da conscientização das pessoas. É fundamental que os colaboradores compreendam a importância de sua

participação na segurança geral da organização, colaborando ativamente para prevenir e mitigar ameaças no dia a dia.

Portanto, qualquer anomalia ou e-mail suspeito fora do padrão das suas atividades deve ser imediatamente reportado à equipe de segurança da organização. Ao fazer isso, você contribuirá para a proteção e defesa da sua empresa.

**Referências Bibliográficas:**

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
**ACADEMY**

FEBRABAN