GRAN CONCURSOS

INFORMÁTICA

Segurança da Informação – Ameaças

Livro Eletrônico

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerente de Produção Digital: Bárbara Guerra

CÓDIGO:
230811467533

MAURÍCIO FRANCESCHINI

Servidor público do TJDFT desde 1999, tendo atuado como supervisor de informática por 8 anos no órgão. Graduado em Ciência da Computação pela UnB, pós-graduado em Governança de TI pela UCB e mestrando pela UnB. É professor de Informática para concursos desde 2008 e ministra também algumas disciplinas da área de TI, com experiência em várias instituições renomadas.

GRAN CONCURSOS

SUMÁRIO

APRESENTAÇÃO

Seja bem-vindo(a) à nossa aula sobre Segurança da Informação - Ameaças!

Na era digital em que vivemos, testemunhamos um crescimento exponencial na quantidade de dados com os quais lidamos diariamente. Enfrentamos o desafio de gerenciar essas informações de modo a protegê-las e mantê-las em segurança, visto que o avanço tecnológico nos trouxe um volume imenso de informações digitais. É nesse contexto que a segurança da informação se torna uma preocupação fundamental.

Nesta aula, estudaremos um tópico muito importante dentro da Segurança da Informação: ameaças.

Acredite, esse é um tema recorrente em editais de concursos. Tentarei explicar de maneira leve e prática para que você gabarite todas as questões!

Estarei aqui do outro lado, mas junto com você nessa caminhada. Ao final desta aula, você estará preparado(a) para resolver questões de concursos sobre esse tema.

Desejo uma excelente aula!

SEGURANÇA DA INFORMAÇÃO – AMEAÇAS

1. INTRODUÇÃO

A internet vem se tornando uma ferramenta indispensável e presente na vida da grande maioria da população mundial, proporcionando inúmeras vantagens. Entretanto, junto com esses benefícios surgem preocupações relacionadas às ameaças que rondam o ambiente online.

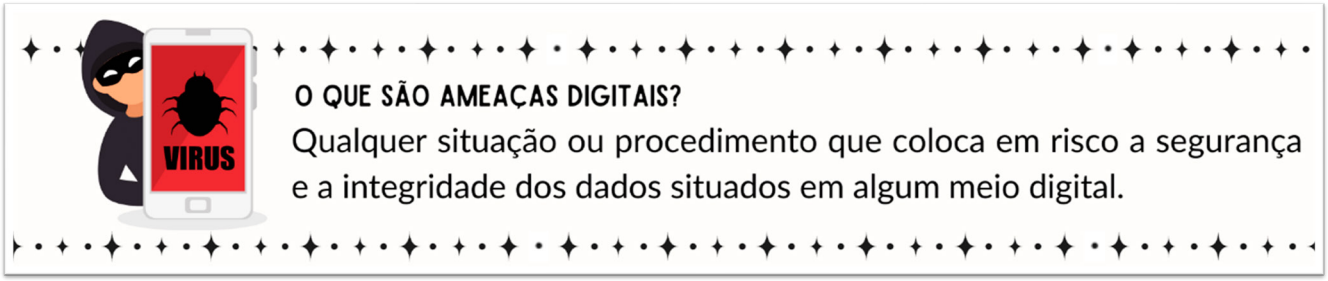
Enquanto nos conectamos com pessoas ao redor do mundo e desfrutamos das oportunidades oferecidas pela internet, devemos ter ciência das ameaças às quais somos expostos quando estamos conectados às redes.

As ameaças estão em constante evolução, e esse é um ponto que não podemos ignorar. Portanto, quanto mais familiarizados estivermos com as possíveis ameaças, mais difícil será para os atacantes causarem danos.

Neste estudo, abordaremos vários tipos de ameaças, como golpes, ataques, malwares e outros riscos que são discutidos em questões de concursos.

O tema **ameaças digitais** engloba diversos conceitos e é uma área dinâmica em constante evolução, com o surgimento frequente de novas ameaças ou o aprimoramento das existentes. Isso resulta em uma imensa variedade de nomenclaturas que precisaremos compreender. Nesta aula, abordarei vários conceitos de forma simples, porém abrangente, sinalizando os tópicos de maior incidência em provas.

1.1. CONCEITO DE AMEAÇAS DIGITAIS

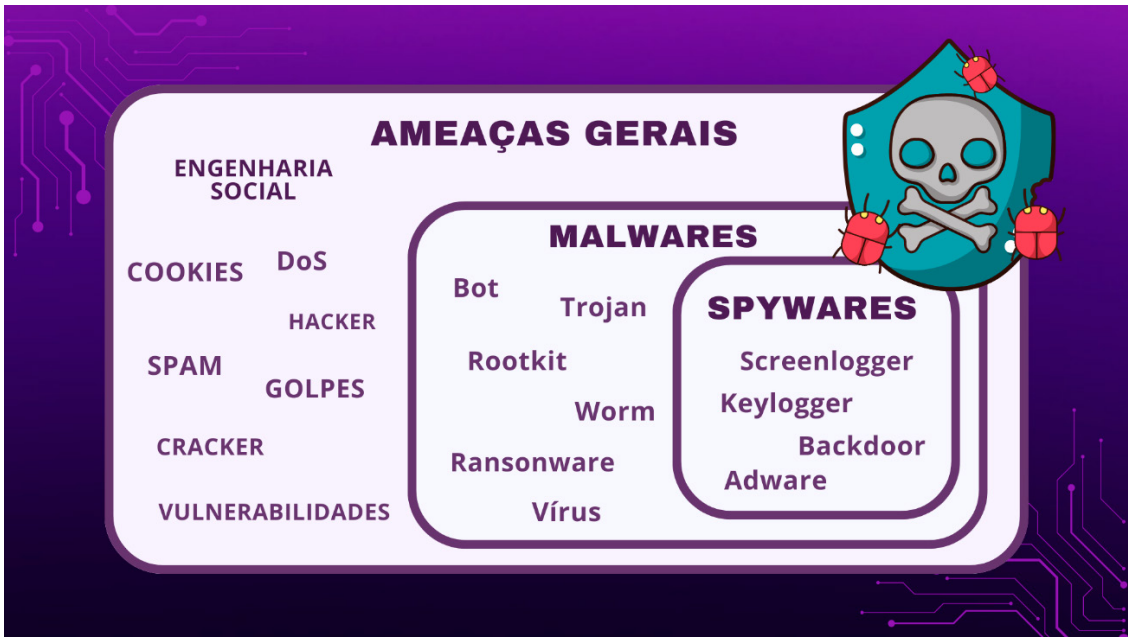


1.1.1. AMEAÇAS DIGITAIS

São quaisquer circunstâncias ou procedimentos que coloquem em risco, causem danos ou comprometam a segurança e a integridade dos dados e sistemas digitais.

Essas ameaças podem ser causadas por indivíduos mal-intencionados, por vulnerabilidades na máquina do usuário, falhas de segurança, entre outros.

Veja, a seguir, o mapa mental das ameaças que criei para que você consiga memorizar e identificar os tipos de ameaças. Não são todas as ameaças existentes, mas com certeza são aquelas que têm maior incidência em provas de concurso.



Podemos classificar as ameaças em ameaças gerais e malwares. Constantemente, nos deparamos com várias formas de fraudes, ataques e golpes nos ambientes computacionais. Vou listar as ameaças campeãs das bancas de concurso e falar sobre como cada uma atua.

ATENÇÃO

Lembre-se de que qualquer situação ou procedimento que coloque em risco, cause danos ou comprometa a segurança ou a integridade dos dados e sistemas digitais é considerado uma ameaça. Portanto, faça a leitura deste mapa mental da seguinte forma: as ameaças englobam tanto as ameaças gerais quanto os malwares e spywares. Isso ficará mais claro no decorrer da nossa aula.

2. AMEAÇAS GERAIS

As ameaças gerais englobam os mais diversos tipos de situações, procedimentos e agentes que causam risco negativo à segurança da informação. Elas não são um software específico, mas sim outros tipos de ameaças, como veremos a seguir.

2.1. HACKER

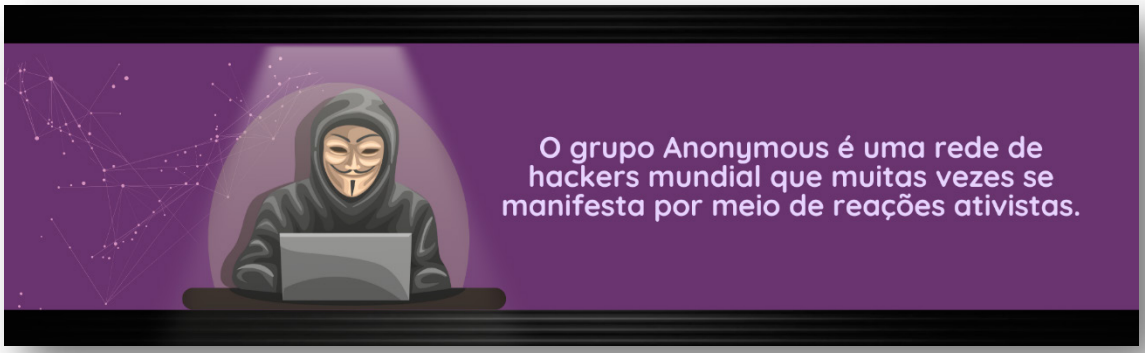
Indivíduo com habilidades cibernéticas, grande conhecimento em programação e segurança digital, e capacidade de invadir dispositivos eletrônicos, sistemas e redes.

Ao contrário do que algumas pessoas pensam, os hackers, em sua grande maioria, não utilizam seus conhecimentos para cometer crimes ou fraudes, mas sim os crackers, que estudaremos logo adiante.

Os hackers podem utilizar suas habilidades de diversas maneiras, seja para exibir seu potencial, explorar curiosidades pessoais ou intelectuais, manifestar-se de forma ativista, política ou ideológica, auxiliar grandes empresas na recuperação de dados ou no aprimoramento de sistemas, entre outros.

Frequentemente, hackers são encontrados em fóruns online, eventos presenciais, reuniões e conferências para debater técnicas de segurança cibernética, compartilhar experiências e auxiliar no desenvolvimento de manuais e mecanismos de proteção no ambiente digital.

Obs.: **Curiosidade:** existe um termo chamado "White hats" ou "hackers do bem", que são os "hackers éticos". O objetivo desses hackers é colaborar nos assuntos de segurança cibernética, corrigindo ou identificando possíveis vulnerabilidades nos sistemas.



Você, em algum momento da sua vida, já deve ter ouvido falar do grupo Anonymous. Esse é um grupo formado por hackers de todo o mundo, que atuam de forma anônima e geralmente se manifestam por meio de reações ativistas, políticas ou ideológicas.

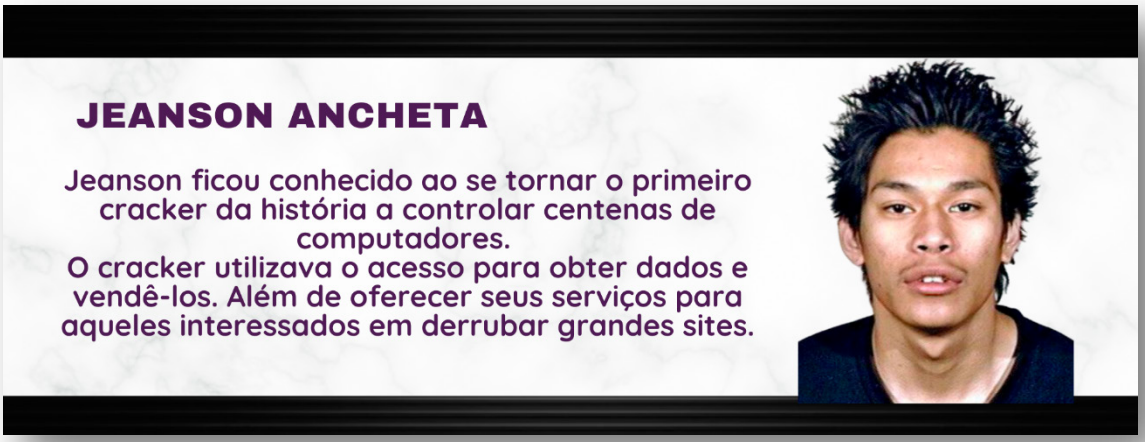
Obs.: Hackers ativistas cibernéticos são chamados de hacktivistas ou ciberativistas.

> **DICA**
>
> **Para fins didáticos, associe o hacker ao "cara legal"; ele não tem a intenção de prejudicar ou causar danos.**

2.2. CRACKER

Indivíduo que possui as mesmas habilidades cibernéticas do hacker, porém com motivações bem diferentes das do hacker. O cracker visa cometer fraudes, furtos, crimes, vandalismos etc.

Veja esse caso:



Para fins didáticos, lembre-se do cracker como o "mau" da história.

Isso quer dizer que a intenção do cracker sempre será causar algum dano, praticar uma fraude ou cometer um crime. Portanto, esse indivíduo não será vinculado a alguém que tenha realizado alguma benfeitoria no ambiente digital.

Obs.: Erradamente, muitas mídias de comunicação veiculam hackers a atividades criminosas no ambiente cibernético, mas lembre-se: esses são os crackers!

2.3. VULNERABILIDADES

São diversas falhas de configuração e funcionamento do sistema que podem criar brechas que permitem o acesso de atacantes. Essas brechas são as vulnerabilidades.

Perceba que, quando estamos falando de vulnerabilidades, não se trata de uma ameaça externa, mas sim de falhas e brechas internas, que acontecem de dentro para fora, possibilitando ou facilitando que invasores mal-intencionados tenham acesso aos computadores, sistemas, dados etc.

Alguns exemplos mais comuns de vulnerabilidades incluem a ausência, desativação ou desatualização do antivírus, a desativação do firewall, a utilização de software pirata, a ausência de backups, a desatualização do sistema operacional e dos softwares em geral.

No entanto, as vulnerabilidades não param por aí: senhas fracas (simples ou curtas) são facilmente descobertas, e a falta de atualizações de segurança e a utilização de dispositivos e redes não confiáveis também são exemplos importantes.

É fundamental compreender que, quando se trata de vulnerabilidades, a causa do dano recai mais sobre o próprio usuário do que sobre o atacante. Infelizmente, a vítima de ataques ou golpes baseados em vulnerabilidades torna-se responsável por não ter tomado todas as medidas de segurança cabíveis para a proteção de seu ambiente digital.

As vulnerabilidades possibilitam diversos tipos de ataques, golpes e malwares que exploram as brechas dos sistemas para se infiltrarem e comprometerem a segurança dos dados e das informações.

Obs.: **Lembre-se: v**ulnerabilidades são brechas no sistema ou ambiente que permitem o acesso de atacantes.

Existe uma vulnerabilidade, bem técnica, na verdade, que é a SQL Injection. Ela é uma vulnerabilidade de segurança que permite que um atacante execute comandos SQL arbitrários em um banco de dados. Isso pode ser feito inserindo código SQL malicioso em um formulário web ou em uma consulta SQL. Uma vez que o código SQL malicioso é executado, o atacante pode obter acesso a dados confidenciais, modificar dados ou até mesmo derrubar o servidor. A SQL Injection é uma das vulnerabilidades de segurança mais comuns em aplicativos web. É estimado que 75% dos aplicativos web são vulneráveis a SQL Injection.

Veja alguns outros exemplos de ameaças que se aproveitam da vulnerabilidade dos sistemas: golpes de phishing, ataques de negação de serviços (DoS), ataques de ransomware, ataques de força bruta, entre outros. Em momento oportuno, falaremos sobre cada um deles.

2.4. SPAM

Mensagem eletrônica **não solicitada**, geralmente enviada em massa para um grande número de pessoas.

Existem vários tipos de spam, como os de propaganda, de boatos (hoax), de golpe e com fins comerciais, entre outros. Os spams mais perigosos são os de golpes, pois são espalhados em massa para atingir o máximo de vítimas possíveis com fraudes, geralmente financeiras.

O spam pode ser inconveniente para os usuários que o recebem. Veja alguns exemplos de como o spam pode afetar os usuários:

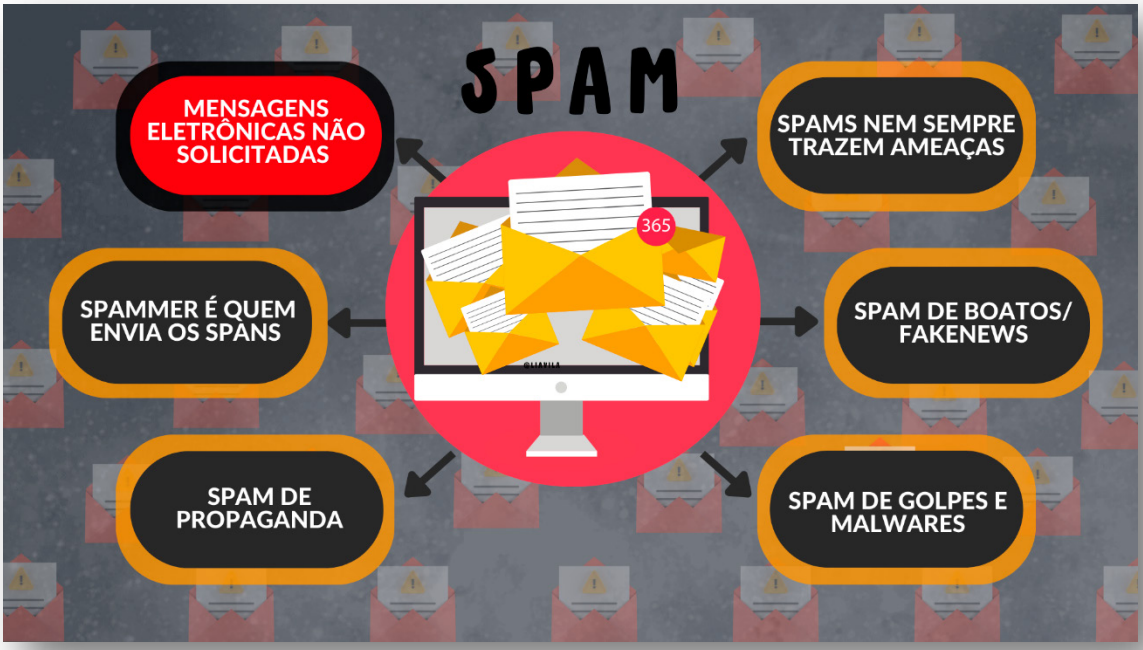
EXEMPLOS

1: pode encher a caixa do usuário impedindo que ele receba e-mails.
2: pode trazer golpes disfarçados no corpo da mensagem.
3: pode conter conteúdo impróprio ou ofensivo.

Obs.: Spams não são apenas mensagens de e-mail; podem ser mensagens de texto por SMS, mensagens de voz em chamadas telefônicas, mensagens no WhatsApp ou qualquer meio eletrônico em que seja possível receber mensagens NÃO SOLICITADAS. Spammer é o indivíduo que envia spams. Ele coleta dados de e-mail utilizando diversas técnicas, dentre elas, a compra de bancos de dados.

O recurso mailing, que é uma lista de distribuição de e-mails, muitas vezes é usado para fazer spams, mas também é utilizado para enviar mensagens de propaganda para aqueles clientes que solicitam e autorizam o envio.

Fake News são notícias falsas propagadas principalmente por redes sociais, sites não confiáveis e aplicativos de mensagens como Telegram e WhatsApp, com a finalidade de manipular e/ou enganar pessoas. Portanto, spams podem trazer fake news.



Obs.: **Lembre-se**: spam são mensagens não solicitadas.

Embora o spam geralmente seja associado ao envio de ameaças, isso não significa que todo spam seja malicioso. Existem spams com finalidade exclusivamente publicitária ou informativa. Mas, ainda assim, são mensagens não solicitadas e muitas vezes inconvenientes.

2.5. ENGENHARIA SOCIAL

Método de ataque que utiliza a persuasão como mecanismo para a obtenção de dados sigilosos do usuário. Esse ataque pode ser realizado por meio eletrônico ou não. Geralmente, o atacante se passa por alguém de confiança, utilizando o nome de instituições conhecidas, como bancos e empresas.

Perceba que essa ameaça **não busca vulnerabilidades de equipamentos**, **sistemas ou redes**; aqui, o atacante busca a vulnerabilidade humana. O intuito do atacante é manipular e enganar a vítima, geralmente buscando obter vantagens pessoais em detrimento dela.

Veja esses exemplos de engenharia social (manipulação e persuasão) associados a golpes ou ataques no ambiente digital.

EXEMPLO

1. Caso hipotético (engenharia social + golpe de phishing)

Fátima recebeu uma mensagem em seu e-mail com texto contendo engenharia social, associado ao golpe de phishing, contendo o seguinte texto:

"Olá! Gostaria de compartilhar uma oportunidade incrível de fazer a diferença na vida das pessoas que mais necessitam da nossa ajuda. Estamos trabalhando incessantemente em um projeto que salvará vidas.

Qualquer ajuda será bem-vinda e você será responsável por devolver a dignidade para crianças que passam fome e vivem na miséria extrema.

Faça parte desse propósito, juntos faremos a diferença! Essas crianças contam com você!"

Link para doação: www.facaparte.com/doaçao

Obs.: É importante ressaltar que existem instituições legítimas que realmente solicitam auxílio e doações de forma transparente e ética. O exemplo anterior foi apenas ilustrativo para demonstrar como funciona a técnica de engenharia social, que pode ser utilizada com diferentes pretextos para enganar usuários e obter benefícios pessoais.

Phishing: usa mensagens de e-mail para persuadir e atrair o usuário. Tal mensagem **contém um link para uma página web falsa**.

2: caso real (engenharia social + catfish)

Catfish: o indivíduo mal-intencionado cria uma identidade falsa e tenta estabelecer uma conexão emocional com a vítima. Após estabelecer a conexão, o atacante manipula as vítimas para realizarem ações que não fariam em circunstâncias normais.

2.6. COOKIES

São arquivos de texto que guardam informações de navegação, autenticação e preferências. Esses arquivos são salvos no computador do usuário pelo site visitado.

ATENÇÃO

Cookies NÃO SÃO VÍRUS, mas sim uma ameaça à privacidade do usuário, pois as informações pessoais de navegação gravadas ali podem ser compartilhadas pelo site visitado com outras empresas ou terceiros.

EXEMPLO

Caso os cookies estejam ativados, ao visitar um site de compra de passagens aéreas e inserir o destino e o período da viagem, suas preferências serão armazenadas. Mesmo que você feche o site, ao abri-lo novamente, os campos já estarão preenchidos com as informações anteriormente fornecidas, facilitando, assim, o processo de busca e reserva de passagens.

2.6.1. PRINCIPAIS TIPOS DE COOKIES

Cookies de sessão: esses cookies são temporários, ou seja, serão utilizados durante uma única sessão de navegação em um site; portanto, quando o usuário fecha o navegador, esses cookies são excluídos automaticamente.

Obs.: Os cookies de sessão são armazenados na memória RAM do computador (temporário) e isso significa que não ficam gravados no disco.

Exemplo de cookies de sessão:

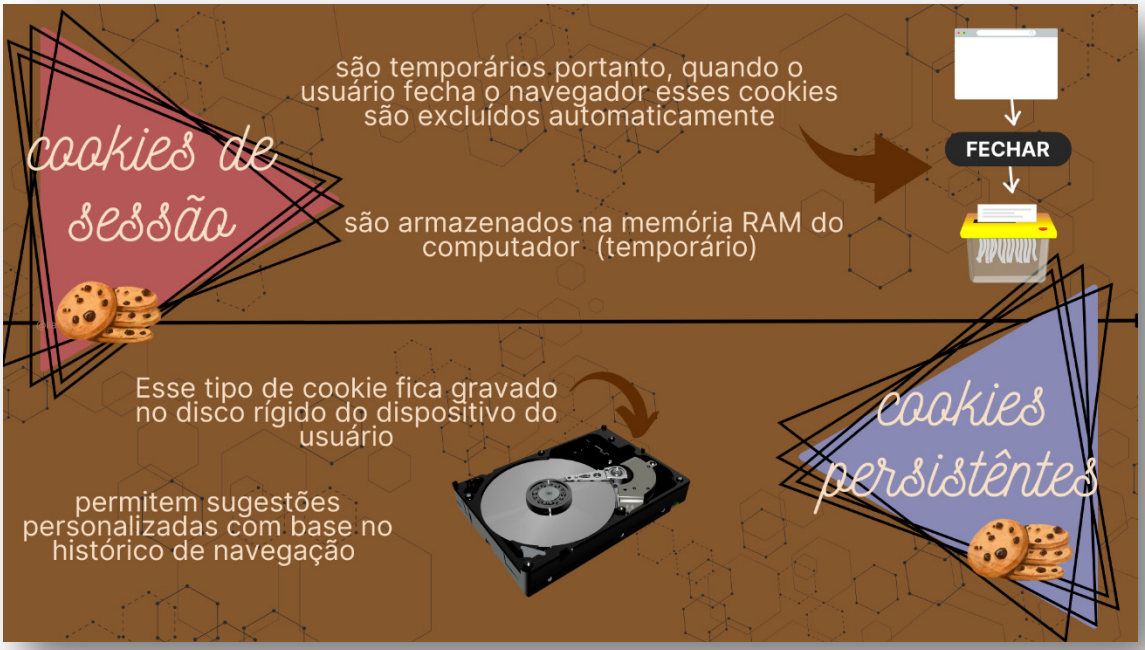
Ao realizar login no website da Amazon, Pedro escolheu e colocou em seu carrinho de compras três livros sobre investimentos e, antes de finalizar a compra, voltou à página inicial do site para escolher outros itens. Apesar de Pedro alternar entre as páginas do site (página inicial e página de finalização de compra), ainda assim a sua sessão permanece ativa no site, ou seja, seu login/senha e os itens escolhidos estarão preservados, sem a necessidade de repetir essas operações. Porém, se Pedro fechar a janela do navegador, todos os dados preenchidos serão excluídos, pois estavam armazenados nos cookies de sessão.

Cookies persistentes: esse tipo de cookie fica gravado no disco rígido do dispositivo do usuário e, independentemente do encerramento da sessão no navegador, permanece no dispositivo com data de expiração definida ou não.

Os cookies persistentes possuem duas funções principais. A primeira está relacionada à autenticação; nesse caso, os cookies verificam se o usuário está conectado e lembram suas informações de login. A segunda trata do rastreamento e significa que os cookies acompanham as visitas ao site, permitindo sugestões personalizadas com base no histórico de navegação.

Exemplos de cookies persistentes:

Armazenamento de informações pessoais, preferências de idioma, histórico de navegação etc. A finalidade desse tipo de cookie é que o usuário tenha uma navegação mais personalizada.



Cookies de terceiros: esse tipo de cookie é gerado por sites distintos daquele que está sendo acessado pelo usuário no momento. Normalmente, eles estão vinculados aos anúncios contidos nas páginas acessadas pelo usuário, permitindo que anunciantes ou empresas de análise acompanhem o histórico de navegação do usuário em vários sites. Por isso, esse cookie é chamado de cookie de rastreamento, pois funciona como se rastreasse a navegação do usuário.

Determinado cookies de terceiros podem assumir a forma de "cookies zumbis". Isso significa que eles permanecem ativos nos dispositivos dos usuários mesmo quando estes optam por não aceitar ou excluir os cookies. Os cookies zumbis são persistentes e difíceis de serem removidos.

Obs.: Cookies zumbis, mesmo após serem excluídos, podem reaparecer.

Os cookies não são os vilões, como você pode ter percebido, visto que não contaminam o computador, sendo geralmente utilizados para melhorar a navegabilidade do usuário. Porém, existem alguns riscos relacionados a eles; vejamos:

- **Coleta e compartilhamento de informações:** os dados coletados pelos cookies podem ser repassados indevidamente para terceiros, o que põe em risco sua privacidade. Por exemplo, quando você faz uma pesquisa sobre pacotes de viagens, ao entrar novamente na internet, você verá vários anúncios sobre isso.

- **Conhecimento de vulnerabilidades:** os cookies podem armazenar dados como informações sobre o sistema operacional ou aplicativos instalados, por exemplo. A partir dessas informações, é possível que um atacante mal-intencionado explore vulnerabilidades no computador.
- **Autenticação automática:** é bem provável que você já tenha marcado a opção "continuar conectado" em algum site; isso significa que as informações de sua conta e login serão armazenadas para autenticação futura. A dica, nesse caso, é que só marque essa opção em dispositivo próprio; caso contrário, pode correr o risco de que outra pessoa faça login no seu lugar.
- **Coleta de informações pessoais**: os dados preenchidos em formulários na web podem ser armazenados em cookies. Nesse caso, o risco é que, se os dados não estiverem criptografados, podem ser coletados por atacantes mal-intencionados e acessados indevidamente.

Terminamos nosso estudo sobre as principais ameaças gerais. A seguir, entraremos no tópico de ataques, que são espécies de ameaças.

3. ATAQUES

Os ataques são ações maliciosas que indivíduos desferem ativamente contra o usuário e seu ambiente. Nesses ataques, há a participação ativa do atacante, seja implantando o ataque para que ele seja executado automaticamente, seja realizando-o diretamente.

3.1. (D)DOS – (DISTRIBUTED) DENIAL OF SERVICE – NEGAÇÃO DE SERVIÇO

É um ataque cibernético que impede o funcionamento do serviço, por meio da sobrecarga do sistema, ocasionada pelo volume excessivo de requisições ao servidor. O objetivo desse ataque é tornar o serviço ou sistema inacessível ao usuário.

Esse ataque também pode ser realizado em massa, atingindo centenas de servidores e sites da internet, o que chamamos de negação de serviço distribuída ou **DDoS**, que é o caso das botnets (redes de bots), que estudaremos quando falarmos de malwares.

Obs.: Essa é uma ameaça que viola o princípio básico da disponibilidade.

ATENÇÃO

Quando falamos em negação de serviço, o objetivo desse ataque é causar indisponibilidade em um site, em um sistema, em uma rede ou na máquina da vítima temporariamente, e não invadir ou coletar informações pessoais. Portanto, não há o que se falar em vazamentos de dados ou contaminação de computadores ou sistemas.

Obs.: Esse ataque explora vulnerabilidades do sistema ou da rede.

Gosto de exemplificar para que você visualize melhor:

EXEMPLO

Quando o site do BBB (Big Brother Brasil) fica indisponível para votação, pode ser um ataque de negação de serviço. Algumas torcidas são muito fortes e podem perder tempo realizando esse tipo de ataque com o objetivo de sobrecarregar os servidores ou torná-los inacessíveis, impedindo que os usuários votem para a eliminação de determinado participante.

Obs.: O termo **SYN Flood** é um exemplo de DoS e já apareceu em prova; vou dar uma breve explicação sobre ele. O **SYN Flood** é um tipo de ataque cibernético com o objetivo de enviar muitas solicitações falsas de conexão para que o servidor fique sobrecarregado, processando as solicitações, o que causa a negação do serviço.

3.2. FORÇA BRUTA (BRUTE FORCE)

Você conhece a expressão "na raça"? O ataque de força bruta é um excelente exemplo dessa expressão.

Esse ataque cibernético consiste em adivinhar o login (nome de usuário) e a senha do usuário por tentativa e erro. O objetivo do atacante é descobrir ou "quebrar" a senha da vítima.

Qualquer tipo de dispositivo ou serviço acessado pela internet que exija login e senha pode sofrer esse tipo de ataque. Novamente, entramos na questão da vulnerabilidade: quanto mais fácil a senha, maior o risco de o atacante adivinhar.

Obs.: Esse ataque explora vulnerabilidades de senhas (fracas, fáceis e curtas).

Vou lhe dar um exemplo de um caso hipotético:

Imagine uma contaem crescimento no Instagram. O usuário demorou 2 anos para alcançar a marca de 250 mil seguidores e, hoje, trabalha exclusivamente com a divulgação de conteúdo digital nessa rede social.

Ao criar a conta, o usuário utilizou os seguintes dados:

Login: @zezim.pensador

Senha: ze1234

Perceba que a senha do nosso usuário fake é fraca, curta e fácil de quebrar*. Nesse caso, o atacante, geralmente utilizando métodos tecnológicos automatizados baseados em tentativas de adivinhação, pode facilmente "adivinhar" o login e a senha do usuário.

Quebrar senha: é o procedimento de obter acesso não autorizado a um sistema, dispositivo ou conta que necessite de senha de acesso.

No caso do nosso exemplo, o atacante, em posse do login e da senha da vítima, pode realizar ações maliciosas se passando pela vítima, alterar a senha para que o usuário não consiga acessar a conta e, portanto, perder seus seguidores e sua ferramenta de trabalho, entrar em contato com fornecedores, aplicar golpes em nome do usuário, dentre outros.

Também pode acontecer de o atacante não descobrir a senha de acesso, mas a plataforma, por possuir um sistema de proteção adequado, entender que está sendo atacada e bloquear a conta, visto a quantidade de tentativas de acesso sem sucesso.

Meu caro aluno(a), se você se viu nessa situação, sugiro fortemente que altere suas senhas, adicionando letras maiúsculas, caracteres e números, de modo a proteger suas contas.

PS: até a criação desta aula, o login do exemplo não estava sendo utilizado por nenhum usuário do Instagram.

3.3. PASSWORD SPRAYING (SPRAYING DE SENHAS)

"Spraying de senhas" é uma técnica de ataque em que um atacante tenta adivinhar a senha de um usuário, testando uma lista de senhas comuns em várias contas. O objetivo do spraying de senhas é obter acesso a contas online, como contas de e-mail, contas bancárias ou contas de mídia social. O spraying de senhas é diferente do ataque de força bruta tradicional porque o atacante não tenta adivinhar a senha de uma conta específica. Em vez disso, o atacante tenta adivinhar a senha de várias contas diferentes, utilizando uma lista de senhas comuns.

O spraying de senhas é uma técnica eficaz porque muitas pessoas usam senhas fracas ou repetem a mesma senha em várias contas. Se um atacante adivinhar a senha de uma única conta, ele poderá acessar todas as outras contas que utilizam a mesma senha.

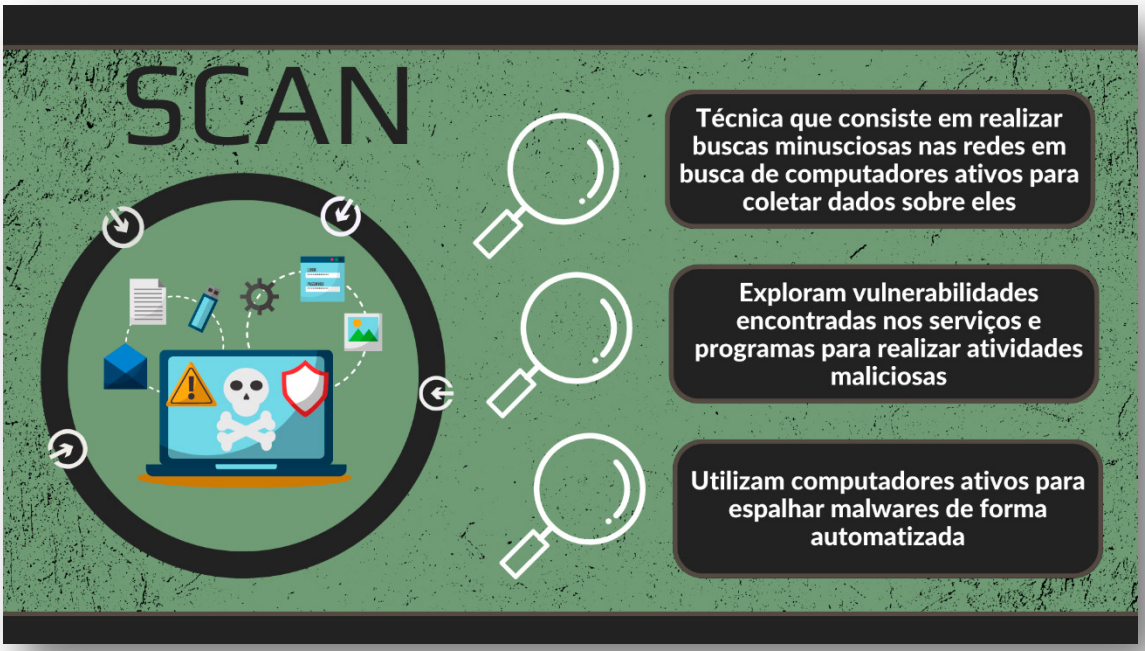
3.4. SCAN

Scan é uma **técnica de varredura** que consiste em identificar hosts ativos (computadores em funcionamento) e possíveis vulnerabilidades no sistema, possibilitando um ataque à vítima.

Obs.: Explora vulnerabilidades no sistema.

Geralmente, essa varredura é feita de maneira automatizada, buscando informações como serviços e programas instalados e, com base nessas informações, procurando brechas no sistema, como a presença de malwares e falhas de segurança, o que facilita a realização de possíveis ataques.

Essa varredura no sistema pode ser benéfica quando realizada de maneira legítima, ou seja, nos casos em que é feita com autorização, com a finalidade de averiguar questões de segurança e, se necessário, realizar as correções ou até mesmo criar medidas preventivas para evitar ataques aos dispositivos ou à rede.



3.5. SPOOFING

É um crime cibernético em que o atacante falsifica sua identidade, "furtando" a identidade de outrem e se passando por ela. Ele pode interceptar a conexão de um usuário a um site de compras e se passar pelo site perante o usuário, além de se passar pelo usuário perante o site de compras. Existe um ataque chamado "Homem-no-meio" ou "Man-In-The-Middle" (M.I.T.M), em inglês, no qual o atacante faz exatamente o que foi explicado anteriormente.

Outra forma de spoofing se dá nos e-mails. Nos ataques de spoofing de e-mail ou falsificação de e-mail, o atacante altera os campos do cabeçalho do e-mail (falsifica) para parecer que foi enviado por uma determinada pessoa, mas, na verdade, é enviado por outra.

ATENÇÃO

Independentemente do tipo de spoofing, todos possuem a mesma finalidade: **falsificar a origem** da mensagem ou dos dados.

ATENÇÃO

Cuidado!

Existe uma distinção entre o golpe de phishing e o ataque de spoofing, sendo que o ataque de spoofing disfarça a origem com o objetivo de parecer ter sido enviado por uma determinada pessoa. Enquanto o golpe de phishing usa engenharia social para persuadir os usuários a clicarem em algum link fraudulento, acreditando ser legítimo, possibilitando o acesso às informações pessoais.

Mas o spoofing e o phishing podem acontecer de maneira simultânea. Veja este exemplo:

Caso hipotético: o atacante, com a finalidade de parecer uma instituição bancária, falsifica o remetente do e-mail, identificando-se com o endereço de um banco legítimo (spoofing). No corpo do e-mail, o atacante direciona o usuário a clicar em algum link fraudulento (phishing).

3.6. SNIFFING (INTERCEPTAÇÃO DE TRÁFEGO)

Sniffer (farejador) é um dispositivo de software ou hardware que permite ao usuário monitorar o tráfego de dados na internet em tempo real.

Dito isto, vamos ao ataque de sniffing. Essa técnica é utilizada por atacantes com o objetivo de capturar, por exemplo, senhas, números de cartão de crédito e conteúdos confidenciais que estejam trafegando em uma rede privada ou pública sem criptografia nas conexões.

Esse ataque funciona da seguinte forma: o atacante "fareja" as conexões da rede e intercepta aquelas não criptografadas, capturando os dados com o objetivo de obter informações do usuário.

Caso hipotético: **C**arlos precisou acessar a rede Wi-Fi aberta do aeroporto, pois sua operadora de celular estava indisponível no momento. Ao acessar essa rede aberta, ou seja, sem criptografia, Carlos ficou exposto aos atacantes que interceptam esse tipo de conexão.

3.7. EXPLOIT

Esse ataque aproveita as vulnerabilidades de um aplicativo, sistema operacional ou até mesmo de hardware para assumir o controle do computador ou roubar dados da rede.

Ele foi criado para aproveitar as brechas, permitindo o acesso indevido e não autorizado do invasor, além de possibilitar o acesso remoto ao sistema, o acesso a informações confidenciais e a interrupção de serviços, entre outros.

Aqui é importante você saber que exploit não é a mesma coisa que vulnerabilidade. O exploit se aproveita das vulnerabilidades existentes em um sistema para realizar o ataque. Por outro lado, a vulnerabilidade é a própria falha, a brecha em si que o exploit explorará.

3.8. DEFACEMENT (DESFIGURAÇÃO DE PÁGINA OU PICHAÇÃO CIBERNÉTICA)

Esse ataque consiste na alteração do conteúdo de um site disponível na web.

O atacante encontra falhas na programação do site, busca vulnerabilidades no servidor onde o site está hospedado, invade o servidor para realizar as alterações desejadas e rouba senhas de acesso remoto para alterar o conteúdo do site.

Esse ataque fere o princípio da integridade, visto que o conteúdo do site é alterado.

Mas qual é a verdadeira finalidade do defacement? Vandalismo! Isso mesmo! Assim como vândalos picham paredes, prédios e casas, no mundo digital, os vândalos também fazem isso, só que em sites, alterando informações, formatações e design para deixá-los desfigurados e deformados.

3.9. SESSION HIJACK

Session hijacking é uma ameaça de segurança cibernética que permite que um atacante assuma o controle de uma sessão de usuário válida em um sistema de computador. Isso pode ser feito roubando o nome de usuário, a senha ou outro identificador de sessão do usuário. Uma vez que o atacante assumiu o controle da sessão, ele pode acessar as informações do usuário, modificar suas configurações ou até mesmo executar ações em seu nome.

O session hijacking pode ser usado para uma variedade de propósitos, incluindo:

- Roubo de identidade
- Fraude financeira
- Espionagem
- Ataques de negação de serviço.

4. GOLPES

Diferentemente dos ataques, os golpes não têm a ação direta do atacante na execução. Ele arma o golpe como uma armadilha e espera que o usuário caia nela. Veremos agora alguns dos golpes cibernéticos mais conhecidos.

4.1. PHISHING

O phishing é um tipo de golpe em que o golpista tem o objetivo de obter dados pessoais e financeiros da vítima. Para isso, ele combina o uso de tecnologia com engenharia social.

Mas como isso funciona?

Esse golpe é realizado por meio do envio de mensagens eletrônicas que se passam por instituições conhecidas, como bancos, sites populares ou empresas. Essas mensagens costumam ser atrativas para o usuário e, geralmente, possuem em seu conteúdo um alerta sobre a não execução dos procedimentos descritos, como, por exemplo, o cancelamento de cartão de crédito ou a inclusão do nome nos serviços de proteção de crédito (SERASA). Esse tipo de alerta tem a finalidade de intimidar e constranger o usuário.

O objetivo desse golpe é "pescar" os dados pessoais e financeiros; por isso, o nome desse golpe é Phishing, que vem da palavra inglesa fishing, que significa pescaria. Para atingir esse objetivo, o golpista induz a possível vítima a clicar no link da mensagem, que a direcionará a uma página falsa com um formulário de preenchimento, no qual serão fornecidos seus dados e coletados pelo golpista.

Obs.: Phishing está relacionado ao recebimento de e-mails, sendo também o termo mais geral para esse tipo de golpe. Porém, ultimamente, as bancas têm cobrado o termo "***smishing***". Ele é a mesma coisa que o phishing, porém o golpe chega por mensagem de texto em celulares, ou seja, por SMS, por isso o nome **SMiS**hing.

Abaixo, segue um exemplo real de smishing, retirado das minhas mensagens de texto do celular. O exemplo ficou um pouco pequeno, mas a mensagem diz:

"Não identificamos o pagamento dos serviços OI. Evite a rescisão do contrato e a inclusão no Serasa. Detalhes: https://din.im/1Nnk4r" ou negocie em www.oi.com.br/negociacao.

Em verde, o atrativo, no caso, a preocupação; em amarelo, o alerta; em cinza, o link que direcionará à página falsa para coleta de dados.

Obs.: Uma das formas de prevenção contra esse tipo de fraude é utilizar mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

4.2. PHARMING

Antes da explicação do golpe de Pharming, preciso explicar o que é o DNS.

DNS é um servidor ou protocolo que traduz endereços URL, por exemplo, www.grancursosonline.com.br, para endereços IP, por exemplo, 192.168.0.1. Ou seja, o DNS permite que seu navegador encontre os sites que você busca na internet.

O Pharming é um outro tipo de phishing. Portanto, é um golpe em que o golpista tem o objetivo de obter os dados pessoais e financeiros da vítima; para isso, ele combina o uso de tecnologia com engenharia social.

O golpe de Pharming, no entanto, e, diferentemente do phishing original, redireciona o usuário por meio do envenenamento do DNS, o qual passa a traduzir endereços URL para IP fraudulento. O usuário digita o endereço de um site na barra de endereços do seu navegador, mas é redirecionado para um site diferente. O site para o qual o usuário é redirecionado geralmente é um site falso, criado pelo atacante para enganar o usuário a digitar suas informações pessoais. O atacante, então, pode usar essas informações para roubar a identidade do usuário, fazer compras em seu nome ou cometer outros crimes.

4.2.1. IMPORTANTE: PHISHING X PHARMING

Como são golpes fáceis de nos confundir, pois ambos possuem características comuns, também é preciso saber distingui-los por meio das características que os diferenciam claramente.

Essa é um pouco repetitiva, mas aqui a intenção é fazer você introjetar as diferenças desses golpes, pois o examinador vai tentar confundi-los exatamente nesse sentido, trocando os conceitos. Portanto, vamos deixar esse tópico bem claro, não apenas para você gabaritar questões sobre isso, mas para fazê-lo de forma consciente e com sorriso no rosto. Bora lá!

Características comuns tanto ao Pharming quanto ao Phishing:

- Visam furtar dados do usuário.
- Imitam instituições conhecidas para ganhar credibilidade.
- Usam páginas web falsas, por meio das quais os dados dos usuários são enviados.

Características distintas entre Pharming e Phishing:

- **Phishing**: usa mensagens de e-mail para persuadir e atrair o usuário. Tal mensagem contém um link para uma página web falsa.
- **Pharming**: redireciona o usuário por meio do envenenamento do DNS, o qual passa a traduzir endereços URL para IP fraudulento. O usuário digita o endereço correto na barra de endereços, mas é redirecionado para um endereço falso, geralmente um site que está armazenado no computador do atacante, para onde os dados digitados pelo usuário serão enviados.

4.3. GOLPE DE MALVERTISING (MALWARE ADVERTISING – ANÚNCIOS MALICIOSOS)

Esse ataque está relacionado à inserção de anúncios maliciosos de propaganda em sites de publicidade legítimos. Para que isso ocorra, os golpistas criam anúncios fraudulentos ou maliciosos e os distribuem como se fossem anúncios legítimos em sites de publicidade, os quais dão visibilidade em diversos outros sites da web.

Obs.: Os sites de publicidade não têm conhecimento de que esses anúncios são maliciosos. Portanto, acredita-se que se tratam de anúncios legítimos.

Essa técnica consiste em veicular anúncios de conteúdo malicioso em diversas páginas da web, de modo que, caso algum usuário clique naquele anúncio ou, em alguns casos mais severos, apenas abra a página que contenha tal anúncio, será direcionado para sites maliciosos, colocando em risco o ambiente computacional do usuário. Além disso, há a possibilidade de instalar malwares no computador.

4.3.1. MALVERTISING X ADWARE

Cuidado para não confundir o ataque de malvertising com adware!

ATENÇÃO

Não confunda!

- **Golpe de malvertising** é uma técnica de distribuição de anúncios fraudulentos em redes de publicidade com o objetivo de enganar os usuários para que sejam direcionados a sites maliciosos ou até mesmo permitam a instalação de malwares.
- **Adware** é um software projetado para exibir uma propaganda que, quando utilizado de maneira maliciosa, pode monitorar o tipo de navegação do usuário e direcionar propagandas de acordo com o seu histórico de navegação.

5. MALWARES

Malware é todo tipo de código executável que tenha uma intenção danosa por trás, como apagar ou corromper arquivos, comprometer o funcionamento do computador, desconfigurar o sistema operacional, desinstalar dispositivos de hardware, realizar fraudes bancárias, entre vários outros males que possa causar.

Vejamos agora os principais tipos de malware, aqueles mais cobrados em provas.

5.1. VÍRUS

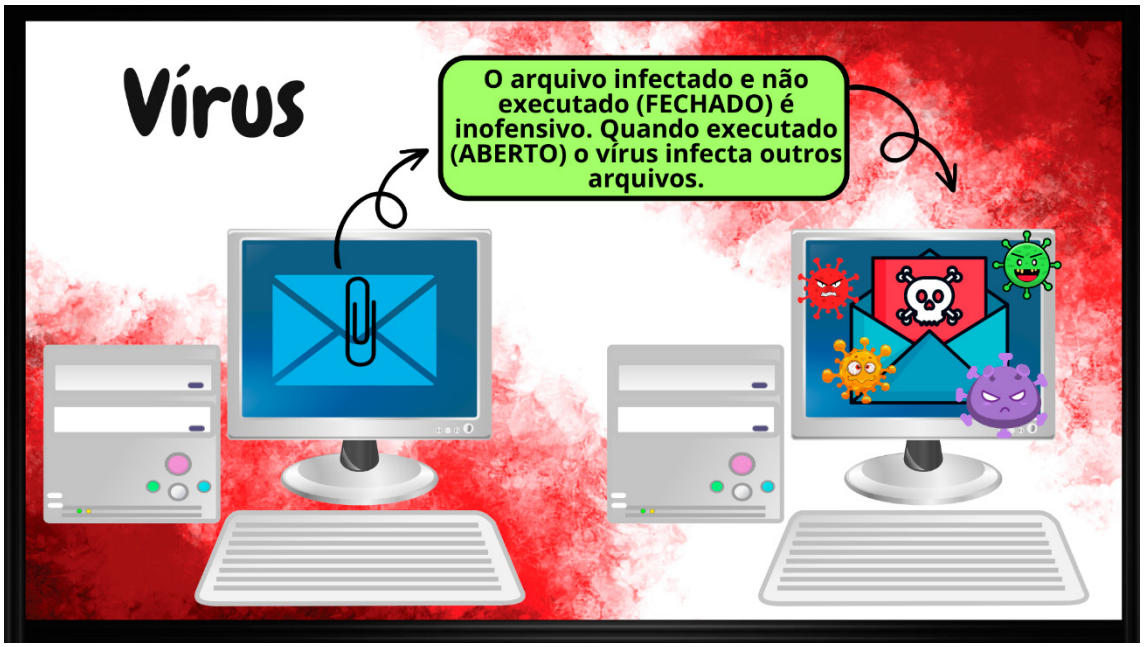
Os vírus de computador são um tipo de malware, ou seja, um código malicioso executável. Eles são desenvolvidos por programadores de software e são inseridos em algum arquivo executável de um programa ou em documentos, como os do Word ou Excel. Esses arquivos são hospedeiros que carregam o código do vírus "inoculado", ou seja, inativo, pois ainda não foram executados. Um arquivo infectado pode permanecer no computador a vida toda e não causar dano algum se não for executado. Porém, ao executar o arquivo infectado, ou seja, ao clicar e abri-lo, o vírus entra em ação e passa a infectar outros arquivos existentes, injetando neles o seu próprio código e se propagando dessa forma.

As principais formas de disseminação dos vírus foram por meio de disquetes, mídias removíveis e pen drives com arquivos contaminados, bem como em sites de downloads e e-mails com arquivos anexos infectados. Essa é a forma como o vírus se replica: infectando outros arquivos existentes no computador. Ele insere cópias de seu código em arquivos existentes. Atenção! Ele não consegue criar uma cópia de si mesmo, mas apenas inserir uma cópia de seu código em outros arquivos.

ATENÇÃO

Vírus não são autônomos, ou seja, precisam ser executados pelo usuário ou por algum meio de ativação externa.

Na maioria das vezes, o usuário é o principal responsável pela contaminação, pois abre arquivos anexos infectados em e-mails sem o devido cuidado, utiliza pen drives infectados de outras máquinas e adota outras práticas negligentes.



Existem diversos tipos de vírus; nesta aula, estudaremos os mais comuns e de maior incidência em provas de concurso.

5.1.1. VÍRUS DE BOOT OU VÍRUS DE INICIALIZAÇÃO

Antes da explicação desse vírus, você precisa saber o que significa "boot". Boot é o processo de inicialização do computador, ou seja, são as ações executadas quando o sistema operacional é iniciado ou reiniciado.

O vírus de boot corrompe os arquivos de inicialização do sistema operacional, impedindo que ele seja iniciado corretamente. Em outras palavras, ele compromete o boot, que é a inicialização do sistema. Portanto, ao falar em vírus de boot, deve-se mencionar a inicialização do sistema.

Os vírus de boot podem:

- Corromper arquivos de inicialização do sistema operacional
- Impedir o carregamento do sistema operacional
- Torna o sistema inutilizável.

5.1.2. VÍRUS DE MACRO

Antes da explicação desse vírus, você precisa saber o que significa ***macro***. Macro é um procedimento automatizado, gravado pelo usuário em arquivos do Office. O objetivo de uma macro é permitir que procedimentos repetitivos sejam realizados automaticamente.

O vírus de macro insere seu código malicioso nos arquivos que possuem macros. Quando o arquivo infectado é executado (aberto), o vírus será ativado junto com a macro, o que implicará na infecção do computador.

Esse tipo de vírus infecta os arquivos do Office que contêm macros. Portanto, ao falar em vírus de macro, devem ser mencionados arquivos do Office.

ATENÇÃO

Geralmente, questões que tratam desse tema devem ser associadas aos arquivos do Office.

5.1.3. VÍRUS STEALTH

É um vírus que se camufla, "escondendo-se" do antivírus durante a varredura da memória, impedindo que este o detecte.

Esse vírus é programado para se esconder nos arquivos do sistema. Para que isso funcione, ele altera suas próprias características ou utiliza técnicas de criptografia para dificultar sua detecção. Dessa forma, pode passar despercebido pelos antivírus, que buscam por padrões conhecidos de códigos maliciosos.

5.1.4. VÍRUS POLIMÓRFICOS

Outro tipo difícil, os vírus polimórficos são vírus mutantes que se escondem mudando de forma. À medida que se replicam, eles criam clones ligeiramente diferentes uns dos outros. Isso ajuda a evitar a detecção, pois torna mais difícil para o sistema imunológico identificar e combater o vírus. Um exemplo é o vírus VirLock, que muda de forma e incorpora alguns elementos típicos de um ransomware, mantendo, porém, sua funcionalidade original.

5.1.5. Vírus Bomba Relógio

Assim como a bomba-relógio da vida real, esse vírus é programado para realizar ações em momento específico ou em condição específica.

Esse tipo de vírus, também conhecido como vírus bomba-relógio, é projetado para causar danos no ambiente digital no momento de sua ativação.

Ao ser ativado, pode executar ações como apagar arquivos, corromper dados e danificar o sistema operacional, entre outros. A finalidade desse malware é causar prejuízos ao usuário.

Uma característica importante é que essa ameaça passa despercebida quando inativa, o que torna mais difícil a sua identificação.

5.2. CAVALO DE TROIA OU TROJAN

O nome Cavalo de Troia faz referência a um episódio da mitologia grega em que os gregos usaram, de forma dissimulada, um enorme cavalo de madeira para invadir a cidade de Troia. Assim como na mitologia grega, o Cavalo de Troia digital é um tipo de malware que se disfarça como um presente ou aplicativo útil, mas traz consigo várias ameaças, como vírus, worms, bots e spywares.

Ao contrário dos vírus, o Cavalo de Troia não se multiplica. Em vez disso, atua como um transporte para essas ameaças se infiltrarem em um sistema. É comum receber Trojans por e-mail, de onde são frequentemente enviados. É importante destacar que, embora sejam prejudiciais, os Trojans não são vírus, mas sim outro tipo de malware.

Esse tipo de malware pode chegar como programas, arquivos anexados em e-mails, atualizações fraudulentas, downloads de fontes não confiáveis, mensagens instantâneas, entre outros. Uma vez que o Trojan é executado, ele abre caminho para todas as ameaças contidas nele.

Gosto de fazer a seguinte analogia: o Trojan é similar a um caminhão de bombeiro furtado para ser utilizado em assaltos. Ninguém imagina que dentro do caminhão de bombeiros haja assaltantes e armas para causar prejuízo a alguém. Da mesma maneira, o Trojan se disfarça de algo confiável, atraente e inofensivo, porém traz consigo ameaças ocultas.

Obs.: O Trojan é criado para fins maliciosos.

Essa analogia é bem grosseira, mas ajuda a visualizar.

Um tipo de trojan é o RAT, ou Remote Access Trojan. Ele é um tipo de malware que permite que um atacante controle remotamente um computador infectado. RATs podem ser usados para uma variedade de propósitos maliciosos, incluindo roubo de dados, espionagem e ataques de negação de serviço.

RATs costumam ser distribuídos por meio de e-mails de phishing, downloads de sites maliciosos ou pela exploração de vulnerabilidades em softwares. Uma vez que um RAT infecta um computador, ele pode ser usado para controlá-lo remotamente, roubar dados, instalar outros malwares ou até mesmo derrubá-lo.

5.3. WORM

O termo worm significa verme, em inglês. Esse tipo de malware é especializado em explorar vulnerabilidades e tem como objetivo causar negação de serviço. Isso significa que esse malware viola o princípio da disponibilidade, pois pode deixar o sistema indisponível.

Uma característica distintiva do worm é a sua capacidade de se autoexecutar e se propagar de forma autônoma, sem depender de um arquivo hospedeiro ou da interação do usuário. Ele se multiplica rapidamente, criando cópias de si mesmo em larga escala, o que compromete significativamente o processamento do ambiente infectado. Essa capacidade de replicação em grande escala o diferencia de outros tipos de malware, como vírus e cavalos de Troia.

Os worms exploram vulnerabilidades das redes e conexões com a finalidade de invadir o ambiente e, uma vez dentro, começam o processo de autorreplicação. No entanto, essa não é a única maneira de invasão; eles podem ser distribuídos por e-mail, links maliciosos, mensagens ou redes compartilhadas.

5.4. BOT

O termo bot é uma abreviação de robot. Ele é utilizado para descrever uma evolução do worm, que é aprimorado com mecanismos de conexão que permitem ao atacante se conectar ao malware e enviar comandos remotos.

É comum chamar o computador infectado por um bot de computador zumbi; isso se dá ao fato de o atacante poder controlar o malware remotamente, sem que o usuário tenha conhecimento.

Da mesma forma que os worms, o bot explora vulnerabilidades das redes e conexões com a finalidade de invadir o ambiente e, uma vez dentro, começa o processo de autorreplicação. No entanto, essa não é a única maneira de invasão; eles podem ser distribuídos por e-mail, links maliciosos, mensagens ou redes compartilhadas.

Após infectado, o computador zumbi pode realizar algumas ações; dentre elas, transformar o computador infectado em um servidor de spams (spam zombies), enviando e-mails em massa.

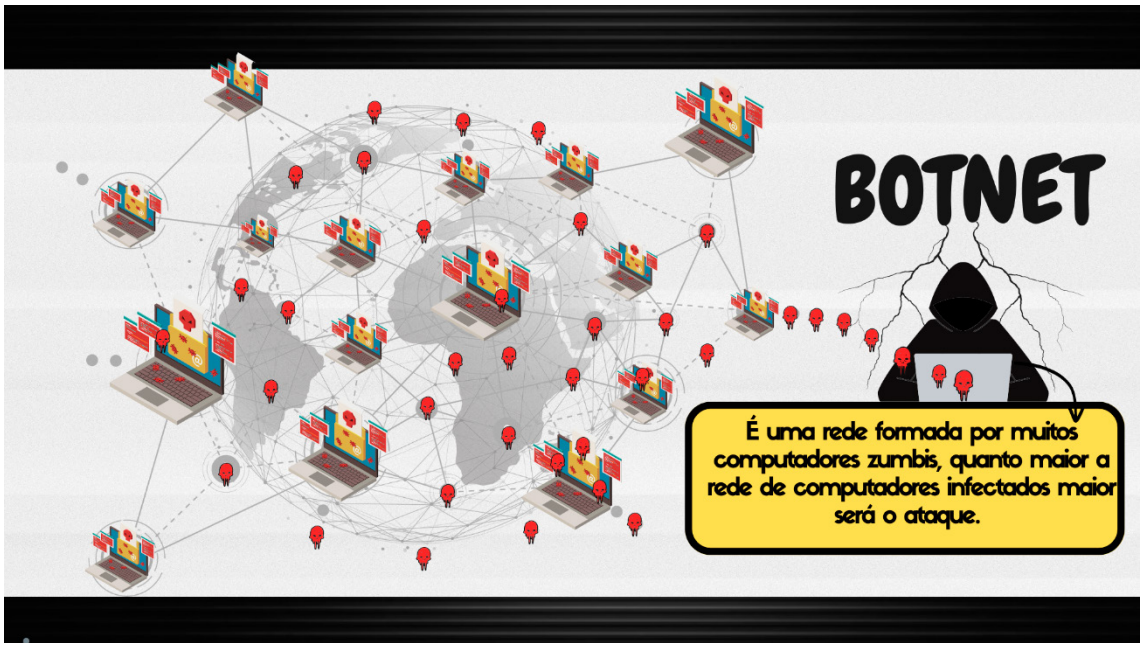
5.5. BOTNET

É uma rede de bots formada por muitos computadores zumbis que desferem ataques em massa. Quanto maior a rede de computadores infectados, maior será o ataque.

Aqui é bem simples: o atacante controla os bots para realizar os ataques. Dentre esses ataques, podem buscar negação de serviço, propagação de malwares, coleta de dados, envio de spam etc.

Funciona da seguinte forma:

O atacante inicia a propagação de bots com o objetivo de infectar o máximo de computadores para transformá-los em computadores zumbis. Os computadores infectados formam uma rede de bots sob o controle do atacante, e os zumbis ficam disponíveis, aguardando as orientações do atacante. Ao término do ataque, os zumbis voltam ao estado de espera até o novo comando.



5.6. RANSOMWARE

É um tipo de malware que sequestra os dados e cobra um valor pelo resgate (ransom), daí a origem do seu nome. Vamos entender como esse sequestro acontece:

O atacante invade o sistema e criptografa os dados da vítima, de maneira que ela não consiga mais acessá-los. O acesso a esses dados fica condicionado ao pagamento da quantia exigida pelo atacante, que, após receber o valor, libera a chave que descriptografa os dados.

Vou contar uma breve experiência de um ataque recente de Ransomware no órgão em que trabalho, o TJDFT.

Esse ataque ocorreu em julho de 2022, quando um atacante invadiu a rede do TJDFT por meio de uma conexão remota, após ter quebrado a senha de um usuário. Na sequência, ele invadiu o servidor da rede e o infectou com Ransomware. Nossa sorte foi ter detectado a ação dele antes que conseguisse criptografar qualquer tipo de dado. No entanto, foi preciso "implodir" toda a rede e os servidores, pois não sabíamos quais haviam sido infectados. Tudo ficou inoperante por uma semana, até fazermos uma varredura completa da rede e dos servidores e restaurarmos o funcionamento básico de cada um deles. Pense no sufoco!!!!

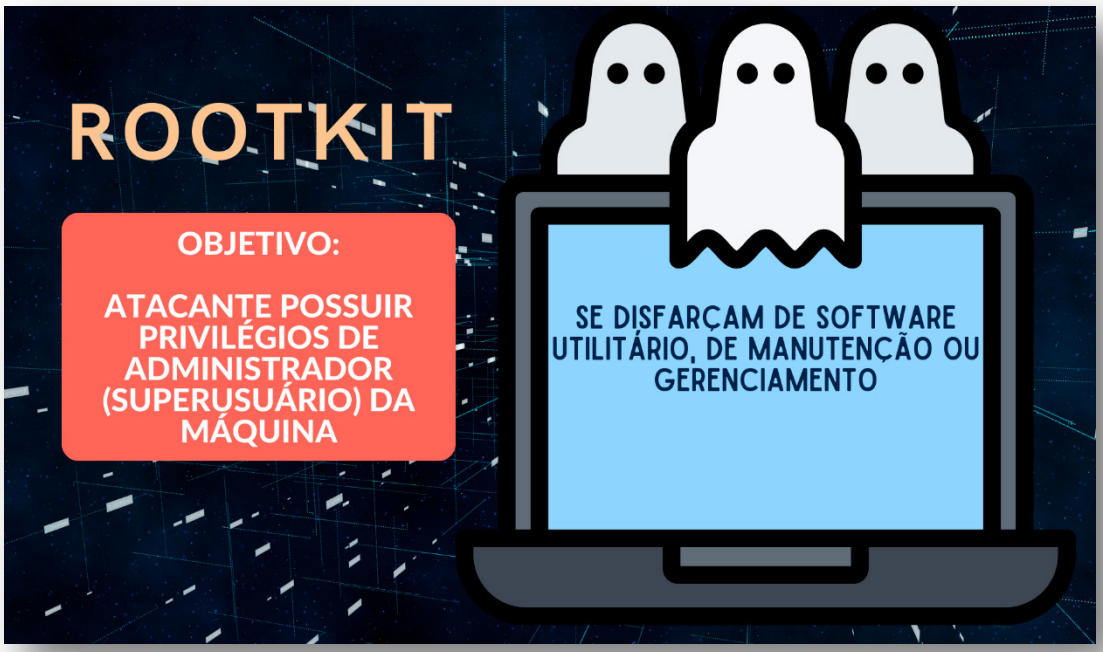
Após esse ataque, estamos reestruturando essa parte da segurança, implementando diversos mecanismos e camadas de proteção. Quis compartilhar com você para melhor visualização desse malware.

5.7. ROOTKIT

De acordo com a Cartilha de Segurança da Informação, o termo rootkit origina-se da junção das palavras "root" (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e "kit" (que corresponde ao conjunto de programas usados para manter os privilégios de acesso dessa conta).

Rootkit refere-se a um conjunto de programas e técnicas utilizadas para esconder e assegurar a permanência do atacante ou até mesmo de outro código malicioso no computador infectado da vítima. Assim, disfarçam-se como um utilitário ou software de manutenção ou gerenciamento, com o objetivo de obter privilégios de administrador (root).

Obs.: Superusuário é a conta com os maiores privilégios e permissões em sistemas operacionais como Linux e Android. Esses privilégios permitem acessar, modificar e controlar tudo no sistema operacional. Devido aos amplos privilégios concedidos à conta de superusuário, ela se torna perigosa quando utilizada por indivíduos mal-intencionados.



5.8. SPYWARE

Spyware é uma categoria de malware que atua como um espião, coletando dados do usuário sem seu conhecimento ou consentimento. Esses tipos de malware são classificados como spywares devido ao seu propósito de capturar informações pessoais sem o conhecimento do usuário. Eles são projetados para operar de forma furtiva, infiltrando-se nos sistemas e monitorando atividades, como registros de digitação, histórico de navegação, senhas e outras informações sensíveis.

O objetivo desses spywares é obter acesso não autorizado aos dados pessoais e utilizá-los para fins maliciosos, como roubo de identidade ou espionagem.

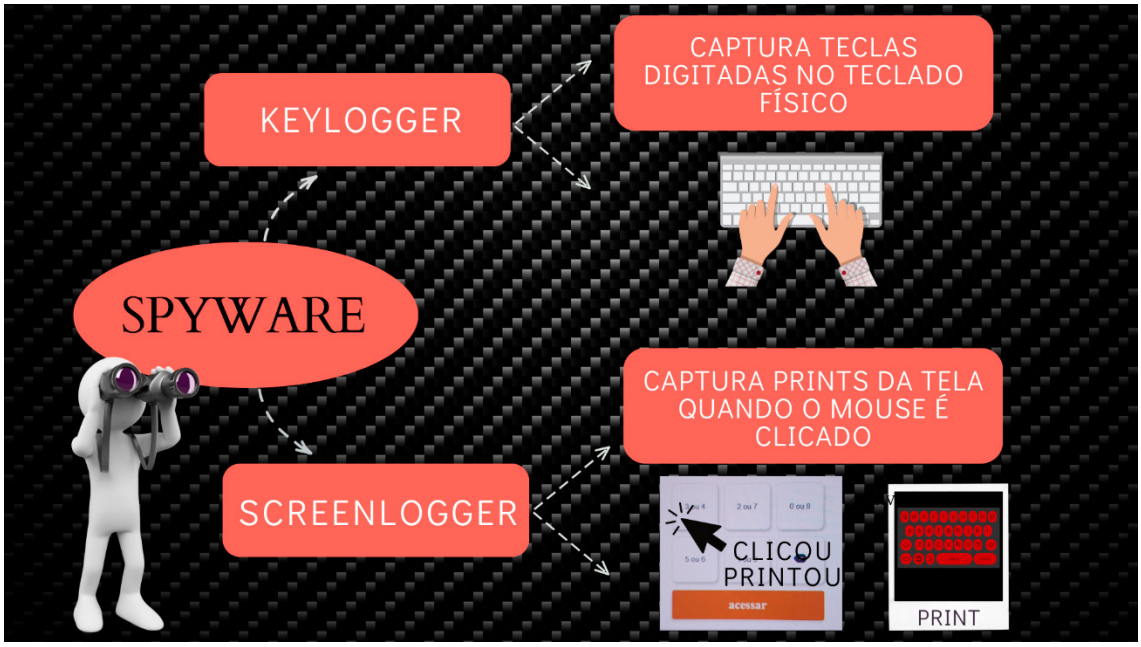
Os próximos malwares que veremos são classificados como spywares, pois têm o objetivo de capturar dados do usuário sem que ele saiba.

5.8.1. KEYLOGGER

É um tipo de spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador. Ele foi muito utilizado logo no surgimento dos bancos na internet, por meio dos quais se realizavam várias fraudes bancárias ao capturar a agência, a conta e a senha que o usuário digitava no teclado físico. Para evitar esse tipo de fraude, foi criado o teclado virtual, que disponibiliza na tela as teclas para serem selecionadas com o mouse.

5.8.2. SCREENLOGGER

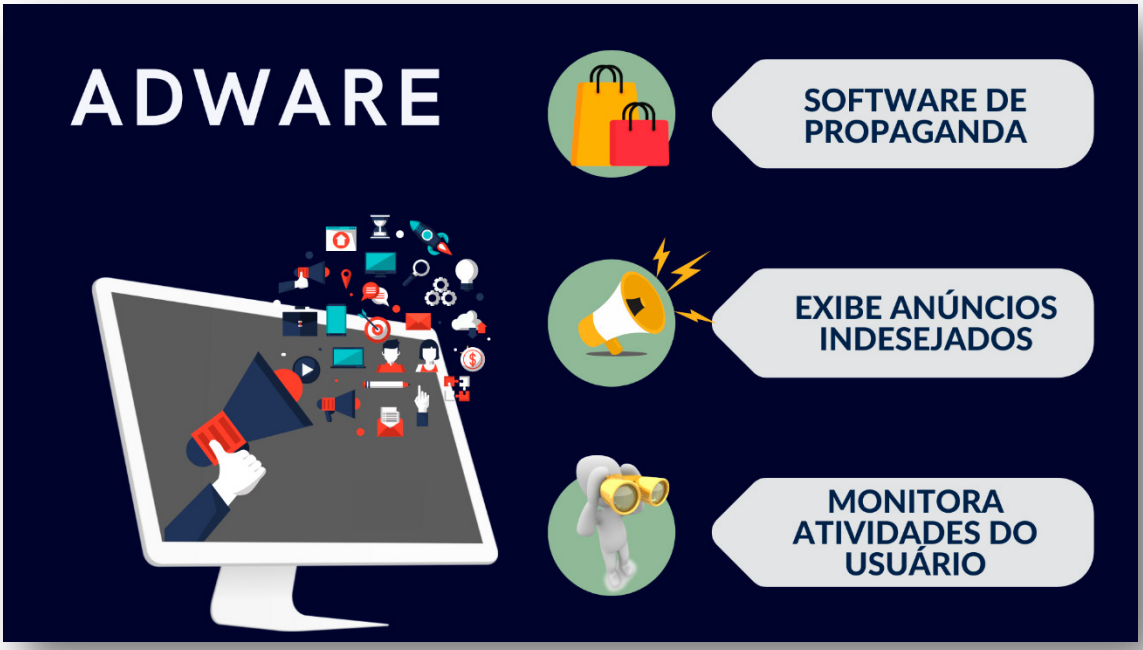
Esse tipo de spyware é uma evolução do Keylogger, e vou te explicar o porquê. Lembra que eu falei que foi criado o teclado virtual para evitar fraudes? Pois é, o screenlogger captura prints da tela quando o mouse é clicado, permitindo que o atacante tenha acesso aos dados contidos na tela printada.



5.8.3. ADWARE

Esse tipo de spyware é projetado para se apresentar como propaganda. Quando utilizado com finalidade maliciosa, esse software passa a monitorar a navegação do usuário sem seu conhecimento e consentimento, direcionando as propagandas de acordo com o tipo de navegação.

Você já deve ter se deparado com aquelas propagandas durante o processo de instalação. Alguns desses softwares são instalados justamente nesse momento, pois é necessário que o usuário informe que não deseja instalar aquele software de propaganda. No entanto, na maioria das vezes, nem lemos o que está escrito e clicamos em “Avançar”. É aí que a ameaça se instala. Uma vez instalado, o usuário nem percebe a existência do software, o qual está, geralmente, rodando em segundo plano e coletando informações do usuário em seu microcomputador.



ATENÇÃO

Não confunda!

- **Adware** é um software projetado para parecer uma propaganda que, quando utilizado de maneira maliciosa, pode monitorar o tipo de navegação do usuário e direcionar propagandas de acordo com o seu histórico de navegação.
- **Golpe de malvertising** é uma técnica de distribuição de anúncios fraudulentos em redes de publicidade com o objetivo de enganar os usuários para que sejam direcionados a sites maliciosos ou até mesmo permitam a instalação de malwares.

5.8.4. BACKDOOR

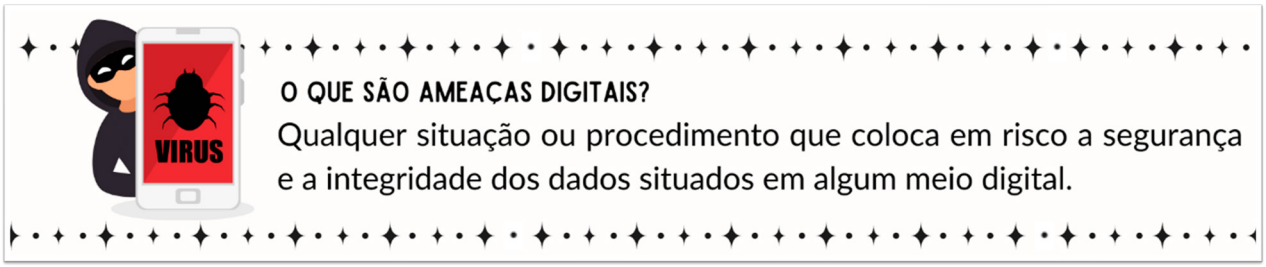
É um tipo de spyware que é instalado na máquina do usuário para abrir brechas para o retorno do invasor.

Como a finalidade do Backdoor é garantir o acesso futuro ao computador comprometido, uma vez instalado, ele permite que o computador seja acessado remotamente. Geralmente, o Backdoor permanece oculto e não é detectado facilmente.

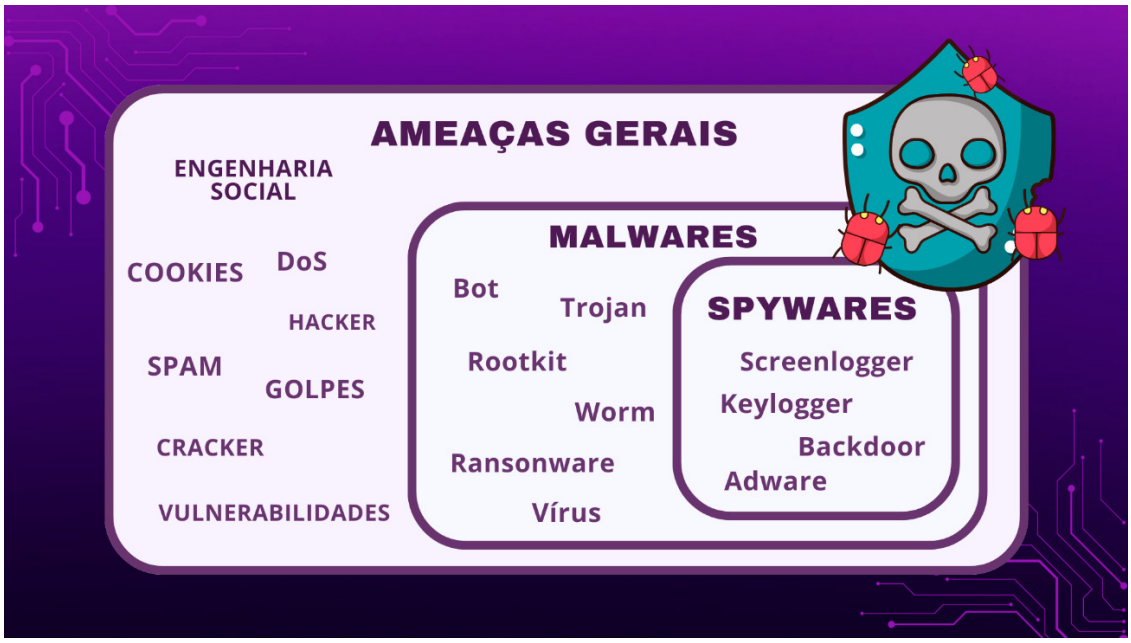
RESUMO

Vamos revisar rapidamente todos os ataques vistos em nossa aula para relembrarmos cada um deles e irmos para a prova afiadíssimos, ok?

CONCEITO DE AMEAÇAS DIGITAIS



Veja, a seguir, o mapa mental das principais ameaças.



AMEAÇAS GERAIS

As ameaças gerais englobam os mais diversos tipos de situações, procedimentos e agentes que causam riscos negativos à segurança da informação.

HACKER

Indivíduo com habilidades cibernéticas, grande conhecimento em programação e segurança digital, e capacidade de invadir dispositivos eletrônicos, sistemas e redes. Exemplo: grupo Anonymous.

CRACKER

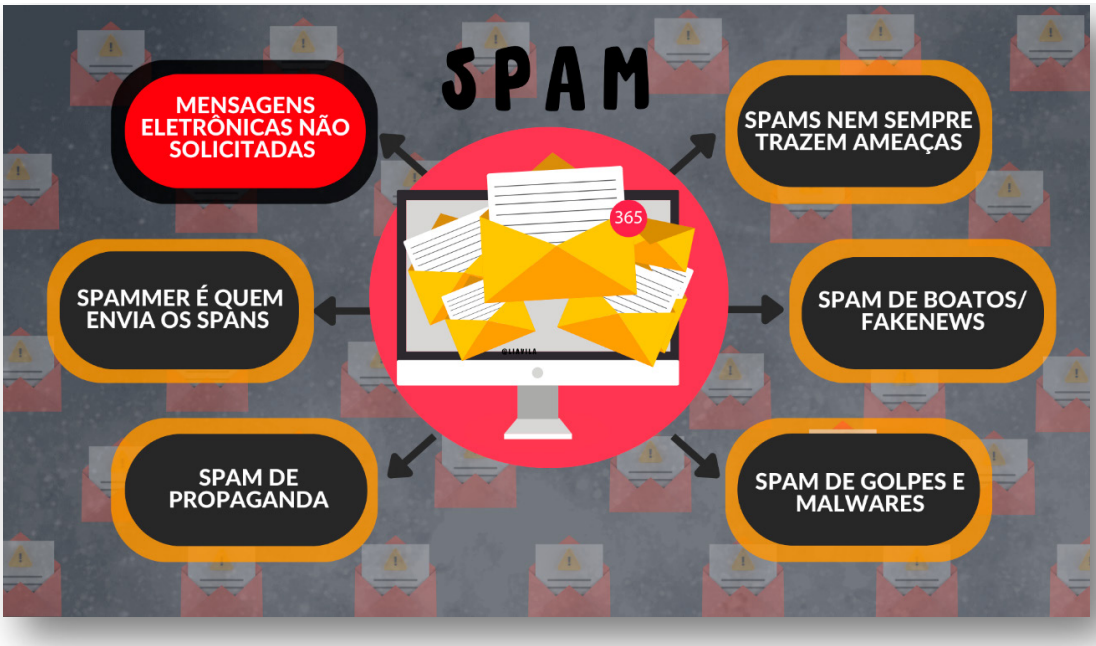
O cracker visa cometer fraudes, furtos, crimes, vandalismos etc. Isso quer dizer que a intenção do cracker sempre será causar algum dano, praticar uma fraude ou um crime.

VULNERABILIDADES

São as diversas falhas de configuração e funcionamento do sistema que podem criar brechas que permitem o acesso de atacantes. Essas brechas são as vulnerabilidades.

SPAM

Mensagem eletrônica **não solicitada**, geralmente enviada em massa para um grande número de pessoas.



Obs.: **Lembre-se**: spam são mensagens não solicitadas.

ENGENHARIA SOCIAL

Método de ataque que utiliza a persuasão como mecanismo para a obtenção de dados sigilosos do usuário.

COOKIES

São arquivos de texto que guardam informações de navegação, autenticação e preferências. Esses arquivos são salvos no computador do usuário pelo site visitado.

ATENÇÃO

Cookies NÃO SÃO VÍRUS!

Terminamos nosso estudo sobre as principais ameaças gerais. A seguir, entraremos no tópico de ataques, que são espécies de ameaças.

ATAQUES

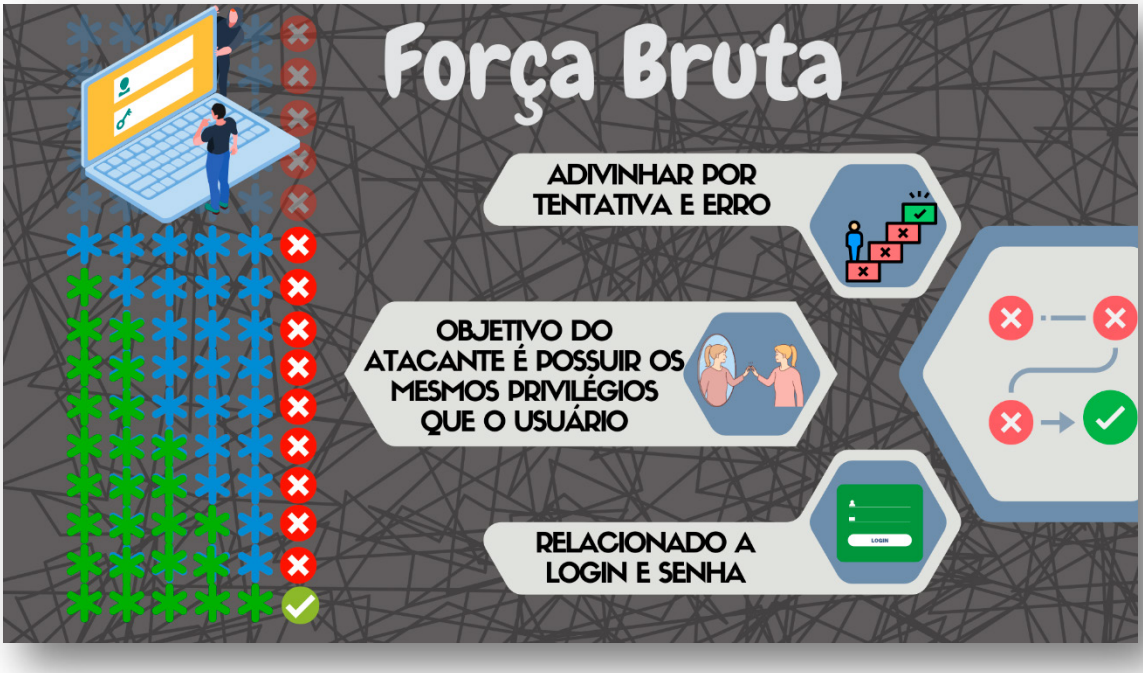
Os ataques são ações maliciosas que indivíduos desferem ativamente contra o usuário e seu ambiente.

D) DOS – (DISTRIBUTED) DENIAL OF SERVICE – NEGAÇÃO DE SERVIÇO

É um ataque cibernético que interrompe o funcionamento do serviço, por meio da sobrecarga do sistema, ocasionada pelo volume excessivo de requisições ao servidor.

FORÇA BRUTA (BRUTE FORCE)

Esse ataque cibernético consiste em adivinhar o login (nome de usuário) e a senha do usuário por tentativa e erro. O objetivo do atacante é descobrir ou "quebrar" a senha da vítima.



PASSWORD SPRAYING (SPRAYING DE SENHAS)

"Spraying de senhas" é uma técnica de ataque em que um atacante tenta adivinhar a senha de um usuário, testando uma lista de senhas comuns e fáceis que as pessoas costumam usar, por exemplo: 123456, senha123, password, data de nascimento, CPF etc. **Scan**.

Scan é uma **técnica de varredura** que consiste em identificar hosts ativos (computadores em funcionamento) e possíveis vulnerabilidades no sistema, possibilitando um ataque à vítima.

SPOOFING

Pode interceptar a conexão de um usuário a um site de compras e se passar pelo site perante o usuário, assim como se passar pelo usuário perante o site de compras. Exemplo: "Homem-no-meio" ou "Man-In-The-Middle" (M.I.T.M), em inglês.

Nos ataques de spoofing de e-mail, o atacante altera os campos do cabeçalho do e-mail (falsifica) para parecer que foi enviado por uma determinada pessoa, mas, na verdade, é enviado por outra.

SNIFFING (INTERCEPTAÇÃO DE TRÁFEGO)

O atacante "fareja" as conexões da rede e intercepta aquelas não criptografadas, capturando os dados com o objetivo de obter informações do usuário.

EXPLOIT

Esse ataque aproveita as vulnerabilidades de um aplicativo, sistema operacional ou até mesmo de hardware para assumir o controle do computador ou roubar dados da rede.

DEFACEMENT (DESFIGURAÇÃO DE PÁGINA OU PICHAÇÃO CIBERNÉTICA)

Esse ataque consiste na alteração do conteúdo de um site disponível na web.

O atacante encontra falhas na programação do site, busca vulnerabilidades no servidor onde o site está hospedado, invade o servidor para realizar as alterações desejadas e rouba senhas de acesso remoto para modificar o conteúdo do site.

SESSION HIJACK

Permite que um atacante assuma o controle de uma sessão de usuário válida em um sistema de computador. Isso pode ser feito roubando o nome de usuário, a senha ou outro identificador de sessão do usuário.

GOLPES

Diferentemente dos ataques, os golpes não têm a ação direta do atacante na execução.

PHISHING

O phishing é um tipo de golpe em que o golpista tem o objetivo de obter dados pessoais e financeiros da vítima. Para isso, ele combina o uso de tecnologia com engenharia social. ***Smishing*** é a mesma coisa que o phishing, porém o golpe chega por mensagem de texto em celulares, ou seja, por SMS, daí o nome **SMiS**hing.

PHARMING

O Pharming é um tipo de phishing que, diferentemente do phishing original, redireciona o usuário por meio do envenenamento do DNS, o qual passa a traduzir endereços URL para IP fraudulento.

GOLPE DE MALVERTISING (MALWARE ADVERTISING – ANÚNCIOS MALICIOSOS)

Esse ataque está relacionado à inserção de anúncios maliciosos de propaganda em sites de publicidade legítimos. Para que isso ocorra, os golpistas criam anúncios fraudulentos ou maliciosos e os distribuem como se fossem anúncios legítimos em sites de publicidade, os quais dão visibilidade em diversos outros sites da web.

MALWARES

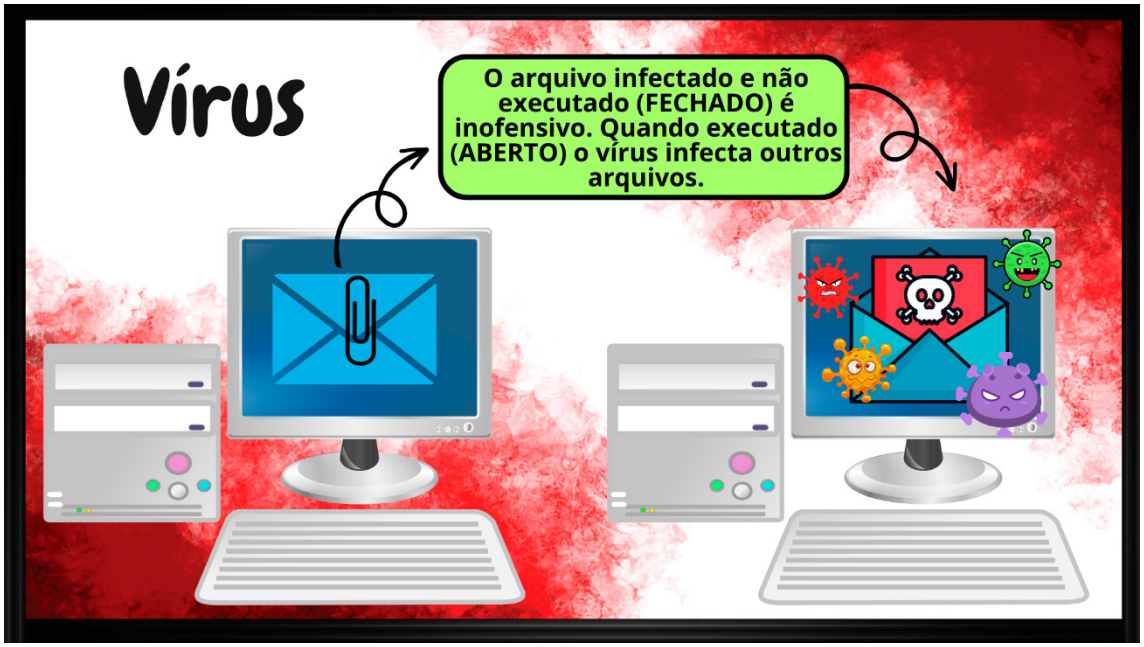
Malware é todo tipo de código executável que tenha uma intenção danosa por trás. Vejamos agora os principais tipos de malware, aqueles mais cobrados em provas.

VÍRUS

Os vírus de computador são um tipo de malware, ou seja, um código malicioso executável. Eles são desenvolvidos por programadores de software e inseridos em arquivos executáveis de programas ou em documentos, como os do Word ou Excel. Esses arquivos são hospedeiros que carregam o código do vírus “inoculado”, ou seja, inativo, pois ainda não foram executados.

ATENÇÃO

Vírus não são autônomos; ou seja, precisam ser executados pelo usuário ou por algum meio de ativação externa.



Existem diversos tipos de vírus; nesta aula, estudaremos os mais comuns e de maior incidência em provas de concurso.

VÍRUS DE BOOT OU VÍRUS DE INICIALIZAÇÃO

O vírus de boot corrompe os arquivos de inicialização do sistema operacional, impedindo que ele seja iniciado corretamente.

VÍRUS DE MACRO

O vírus de macro insere seu código malicioso nos arquivos que possuem macros. Quando o arquivo infectado é executado (aberto), o vírus será ativado junto com a macro, o que implicará na infecção do computador.

VÍRUS STEALTH

Esse vírus é programado para se camuflar e se esconder nos arquivos do sistema. Para que isso funcione, ele altera suas próprias características ou utiliza técnicas de criptografia para dificultar a sua detecção.

VÍRUS POLIMÓRFICOS

Outro tipo difícil, os vírus polimórficos são vírus mutantes que se escondem mudando de forma. À medida que se replicam, eles criam clones que são ligeiramente diferentes uns dos outros. Isso ajuda a evitar a detecção.

VÍRUS BOMBA RELÓGIO

Assim como a bomba-relógio da vida real, esse vírus é programado para realizar ações em momento específico ou condição específica. É um vírus programado para ser executado em uma data e hora específicos. Ao ser ativado, pode executar ações como apagar arquivos, corromper dados e causar danos ao sistema operacional, entre outros. A finalidade desse malware é causar prejuízos ao usuário.

CAVALO DE TROIA OU TROJAN

Assim como na mitologia grega, o Cavalo de Troia digital é um tipo de malware que se disfarça como um presente ou aplicativo útil, mas traz consigo várias ameaças, como vírus, worms, bots e spywares.

WORM

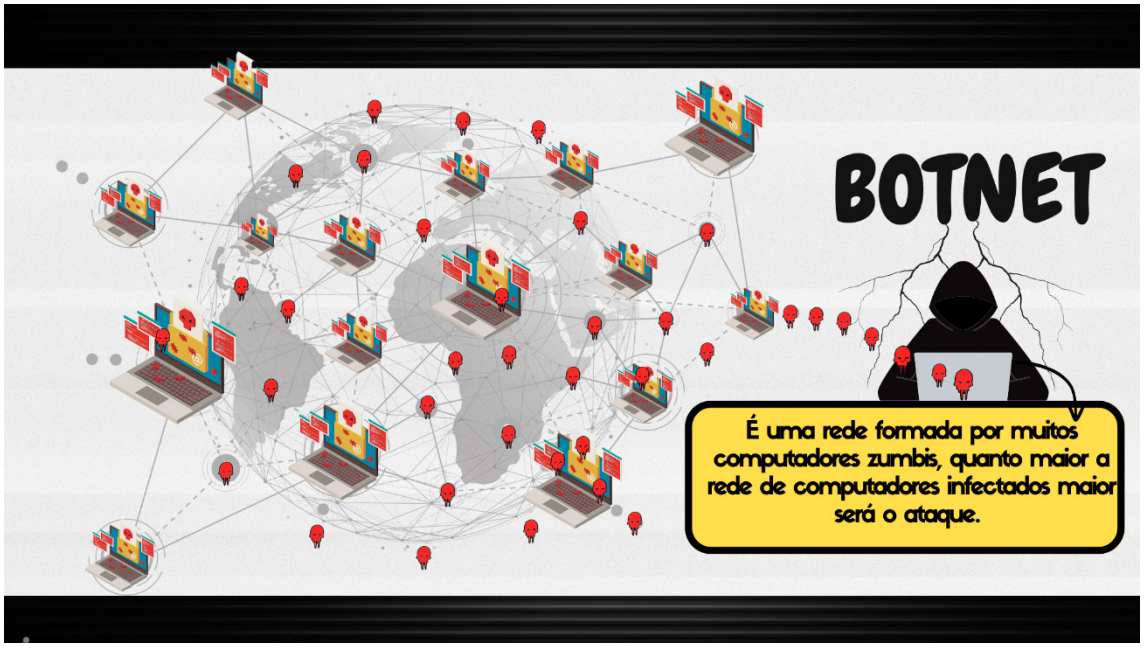
Esse tipo de malware é especializado em explorar vulnerabilidades e tem como objetivo causar negação de serviço. Uma característica distintiva do worm é a sua capacidade de se autoexecutar e se propagar de forma autônoma, sem depender de um arquivo hospedeiro ou da interação do usuário.

BOT

O termo bot é uma abreviação de robot. Ele é utilizado para descrever uma evolução do worm, que é aprimorado com mecanismos de conexão que permitem ao atacante se conectar ao malware e enviar comandos remotos.

BOTNET

É uma rede de bots formada por muitos computadores zumbis que desferem ataques em massa. Quanto maior a rede de computadores infectados, mais intenso será o ataque.

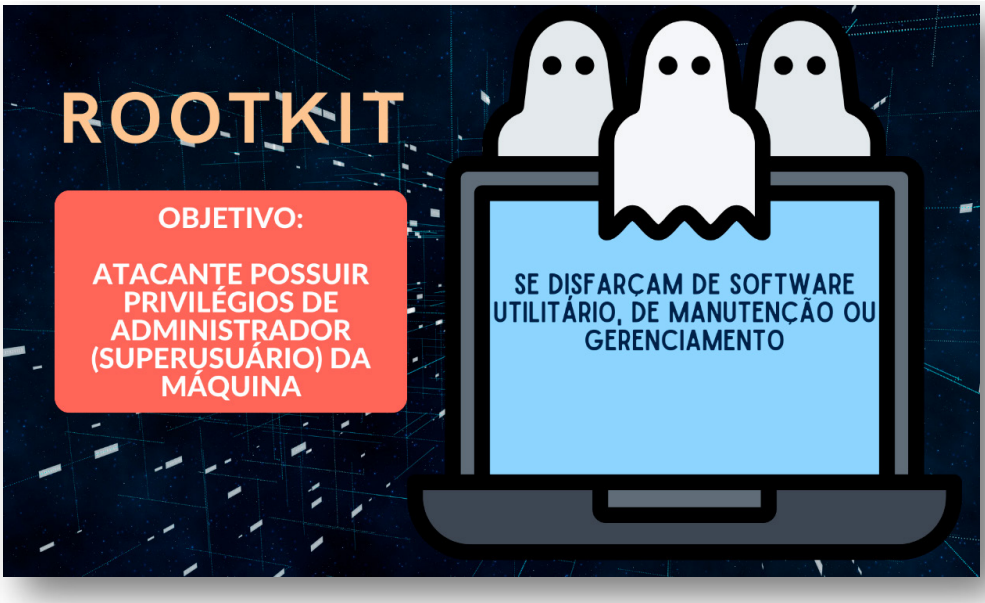


RANSOMWARE

É um tipo de malware que sequestra e criptografa os dados da vítima, cobrando um valor pelo resgate (ransom), daí a origem do seu nome. Vamos entender como esse sequestro acontece:

ROOTKIT

De acordo com a Cartilha de Segurança da Informação, o termo rootkit origina-se da junção das palavras “root” (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e “kit” (que corresponde ao conjunto de programas usados para manter os privilégios de acesso dessa conta).



SPYWARE

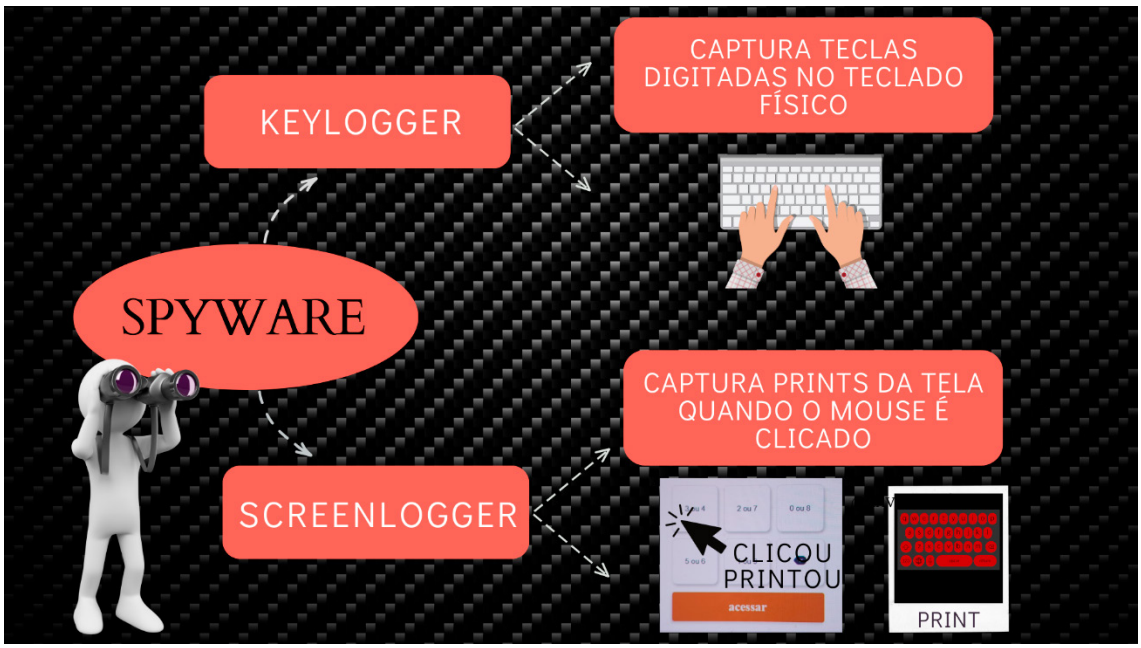
Spyware é uma categoria de malware que atua como um espião, coletando dados do usuário sem seu conhecimento ou consentimento.

KEYLOGGER

É um tipo de spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador.

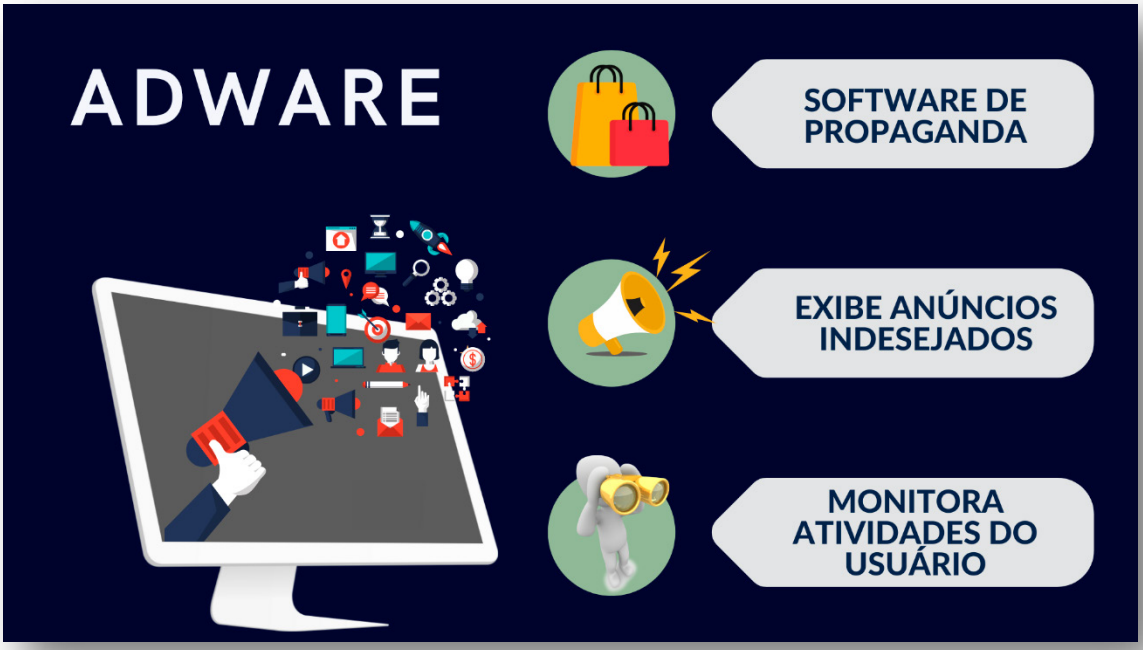
SCREENLOGGER

O screenlogger captura prints da tela quando o mouse é clicado, permitindo que o atacante tenha acesso aos dados contidos na tela printada.



ADWARE

Esse tipo de spyware é projetado para se apresentar como propaganda. Quando utilizado com finalidade maliciosa, esse software passa a monitorar a navegação do usuário sem seu conhecimento e consentimento, direcionando as propagandas de acordo com o tipo de navegação.



BACKDOOR

É um tipo de spyware que é instalado na máquina do usuário para abrir brechas para o retorno do invasor.

QUESTÕES DE CONCURSO

Agora que você conseguiu finalizar a parte teórica, vamos praticar a fundo tudo aquilo que foi visto, mas com muitas questões. Muito bem, foram selecionadas 50 questões de diferentes bancas muito conceituadas no mundo dos concursos. Todas as questões foram extraídas do nosso site Gran Questões, *https://questoes.grancursosonline.com.br/*, e possuem um identificador ou ID, por meio do qual é possível localizá-las pelo campo Pesquisar. Faça bom proveito dessa incrível ferramenta que a Assinatura Ilimitada oferece a você.

Primeiramente, trarei as questões para você resolvê-las. Logo após a bateria de questões, teremos o seu gabarito e, em seguida, cada uma delas comentada com minha explicação, na qual procurei ser o mais minucioso possível para que não reste nenhuma dúvida e você nem precise voltar ao caderno de teoria. Mas, se ainda assim você ficar com dúvida, não tem problema: é só me procurar no fórum de dúvidas que eu vou te responder o mais rápido possível.

Se quiser estar um pouco mais próximo de mim, venha para minha rede social no Instagram, ***@prof.mauriciofranceschini*** ou aponte a câmera do seu celular para o QR-Code abaixo. E, se quiser fazer o meu curso completaço, você pode apontar para o outro QR-Code à direita, no qual encontrará todas as matérias de Informática e Direito Digital, como LGPD, LAI, Marco Civil da Internet, SEI e tantas outras aulas. Te espero lá para me dizer quantas questões deste caderno você gabaritou, ok?

Bom, sem mais delongas, mão na massa! Tenha um excelente desempenho!

001. (Q2681739/FEPESE/PREF. PINHALZINHO/PROF. INFORMÁTICA/2023/ADAPTADA) As tentativas ofensivas dos hackers de penetrar em redes e sistemas a fim de causar danos ou roubar dados são chamadas de ameaças virtuais. Assinale a alternativa que descreve corretamente o tipo de ameaça e sua definição.
a) O Ransomware é um programa que permite que uma pessoa controle um computador infectado a distância.
b) O Kidnapper é um programa que sequestra os arquivos e dados de um usuário, com a ameaça de apagá-los, a menos que um resgate seja pago.
c) O Cavalo de Troia (Trojan) é um programa que recolhe informações sobre o usuário e transmite essa informação a uma entidade externa. Pode ser usado para roubar dados bancários, por exemplo.
d) O vírus é um programa que se prende a um arquivo limpo. A partir disso, ele se espalha pelo sistema de computadores, infectando arquivos com algum código malicioso.
e) O worm (verme) é um programa de computador autorreplicante que infecta um programa para se propagar; além disso, pode ser projetado para tomar ações maliciosas tais como deletar um arquivo ou mandar um email.

002. (Q2733022/QUADRIX/CREF 3/JORNALISTA/2023) Julgue os itens, relativos aos conceitos de organização e de gerenciamento de arquivos, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup.
Os vírus não são considerados programas maliciosos, pois são criados pelos crackers, e não pelos hackers.

003. (Q2733017/QUADRIX/CREF 3/ANALISTA TI/2023 (FACIL))Julgue os itens, relativos aos conceitos de organização e de gerenciamento de arquivos, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup.
Códigos maliciosos podem executar ações danosas e atividades maliciosas em equipamentos como roteadores.

004. (Q2732571/OBJETIVA CONCURSOS/PREF. SAGRADA FAMÍLIA/MONITOR DE ENSINO/2023) Adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome desse usuário e com os mesmos privilégios dele é uma clássica técnica utilizada por indivíduos mal-intencionados. Essa técnica é popularmente conhecida como:
a) Scan
b) Spoofing
c) Sniffing
d) Malware
e) Brute force

005. (Q2828627/GUALIMP/PREF. BOM JARDIM/PROFESSOR II/ÁREA HISTÓRIA/2023) Existe uma prática ilícita onde usuários de internet são levados a revelarem informações pessoais, como senhas de cartão de crédito ou informações bancárias, ao acessarem sites que parecem legítimos. Essa prática é chamada de:
a) Extorsão.
b) Ransomware.
c) Phishing.
d) Trojan.

006. (Q2825373/QUADRIX/CREFONO 2/ASSISTENTE DE COMPRAS/2023) Acerca do programa de correio eletrônico Microsoft Outlook, versão web, dos conceitos de organização e de gerenciamento de programas, bem como das noções de vírus, de worms e de pragas virtuais, julgue os itens.
O phishing é uma técnica de engenharia social em que os criminosos se passam por empresas ou por pessoas confiáveis para a obtenção de informações pessoais ou financeiras das vítimas.

007. (Q2706739/FUNDEP/PREF. BARRA LONGA/ASSISTENTE SOCIAL/CRAS/2023) Um Trojan, também conhecido como Cavalo de Troia, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas. Um Trojan pode ser obtido das seguintes maneiras, exceto:
a) A partir de um e-mail.
b) Por meio de compartilhamento de arquivos.
c) Por meio de mensagens instantâneas.
d) De forma automática pela rede.

008. (Q2693421/OBJETIVA CONCURSOS/PREF. SÃO JOSÉ DO INHACORÁ/AGENTE EDUCACIONAL/2023) Phishing, phishing-scam ou phishing/scam é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social. Com relação ao phishing, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

( ) O phishing geralmente ocorre por meio do envio de mensagens eletrônicas.
( ) O fraudador tenta se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular.
( ) Uma das formas de prevenção contra esse tipo de fraude é utilizar mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

a) C – C – C
b) E – E – C
c) C – E – E
d) E – C – C

009. (Q2720449/FUNDEP/PREF. URUCÂNIA/AUXILIAR ADMINISTRATIVO/2023) Hoje em dia, há vários ataques a informações na internet. Conforme o cert.br, a técnica que consiste em efetuar buscas minuciosas nas redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles, é chamada de
a) Sniffing.
b) Brute force.
c) Scan.
d) DDoS.

010. (Q2687166/FUNDAÇÃO CEFETMINAS/PREF. CONTAGEM/AGENTE FAZENDÁRIO/2023) O programa malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário é denominado
a) Spam
b) Adware
c) Keylogger
d) Screenlogger
e) Ransomware

011. (Q2866736/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA: TÉCNICO ADMINISTRATIVO/2023 (FACIL))No que diz respeito ao programa de navegação Mozilla Firefox, em sua versão mais atual, aos procedimentos de segurança da informação e às noções de vírus, worms e pragas virtuais, julgue os itens.
Os vírus de computador não representam uma ameaça à segurança da informação, uma vez que a finalidade deles é apenas o comprometimento do desempenho do computador.

012. (Q2723361/GUALIMP/PREF. DIVINO/ASSISTENTE ADMINISTRATIVO/2023) "Quem navega bastante pela Internet costuma fazer compras em lojas virtuais e, atraído pela promessa de descontos, acaba baixando o Jollywallet. [...] Jollywallet exibe anúncios no computador do usuário e se conecta à web em segundo plano. Criado pela Media Radyoos, o aplicativo é instalado como um add-on (complemento/extensão) para navegadores e também aplica um botão ao lado da caixa de endereços, para acessá-lo rapidamente."

(Fonte: https://www.techtudo.com.br/noticias/2014/02/como-remover-o-jollywallet-do-computador.ghtml).

Pela descrição acima, o Jollywallet é classificado como um:
a) Adware
b) Trojan
c) Ransomware
d) Worm

013. (Q2731752/QUADRIX/CRESS AL/ASSISTENTE TÉCNICO ADMINISTRATIVO/2023) Quanto aos conceitos de organização e de gerenciamento de arquivos, pastas e programas, aos procedimentos de segurança da informação e aos procedimentos de backup, julgue os itens.
A engenharia social é o ataque mais difícil de ser identificado, logo não há como preveni-lo.

014. (Q2791834/FUNDAÇÃO CEFETMINAS/IFSULDEMINAS/MÉDICO/ÁREA CLÍNICA GERAL/2023) Qual é o tipo de fraude de internet por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social, via mensagens eletrônicas?
a) Phishing
b) Advance fee fraud
c) Identity theft
d) Fake news
e) Spyware

015. (Q2824947/INSTITUTO AOCP/PM-DF/2º TENENTE/ÁREA: ADMINISTRAÇÃO/2023) Considerando o comportamento de softwares maliciosos, um BOT é um programa similar a um WORM. A característica específica que diferencia um BOT de um WORM é o fato de o
a) BOT oferecer recursos de captura de teclas digitadas em um teclado virtual.
b) BOT ser projetado para monitorar as atividades em um computador e enviar as informações coletadas para o invasor.
c) BOT ser um programa que torna indisponíveis os dados em um computador, a fim de exigir pagamento de resgate para a restauração do acesso para o usuário.
d) BOT possuir recursos de comunicação com o invasor que permite que o computador infectado seja remotamente controlado.
e) BOT poder ser utilizado por um invasor para apresentar propagandas na tela do usuário, a fim de gerar monetização a partir do acesso às propagandas.

016. (Q2822437/QUADRIX/CRO-PB/AGENTE ADMINISTRATIVO/2023) No que se refere ao programa de navegação Mozilla Firefox, em sua versão mais recente, ao programa de correio eletrônico Microsoft Outlook e às noções de vírus de computador, julgue os itens.
Os vírus de computador não possuem capacidade para tornar o sistema operacional inoperante.

017. (Q2672798/INSTITUTO AVALIA/PREF. SANT'ANA DO LIVRAMENTO/ANALISTA JUDICIÁRIO/2023) Assinale a alternativa que apresenta um tipo de malware que parece ser um programa inofensivo, porém, quando ativado, realiza a abertura de backdoors.

a) Rootkit
b) Cavalo de Troia
c) Bombas-relógio
d) Vírus
e) Spywares

018. (Q2684981/QUADRIX/CRO/AGENTE FISCAL/2023) Considerando o programa de navegação Mozilla Firefox, sítios de busca na Internet e noções de malwares e outras pragas virtuais, julgue os itens de 34 a 37.

Os ataques de malvertising acontecem quando cibercriminosos introduzem anúncios malignos em redes de publicidade online.

019. (Q2793774/COTEC/FADENOR/PREF. FRANCISCO SÁ/ANALISTA FAZENDÁRIO/2023) Considere as seguintes características aplicáveis a malwares:

I – Projetado especificamente para apresentar propagandas, ele pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro, e para fins maliciosos, quando as propagandas apresentadas são redirecionadas sem conhecimento do usuário.

II – Capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador, a sua ativação, em muitos casos, está condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking, por exemplo.

III – Tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, ele exige pagamento de resgate para restabelecer o acesso ao usuário, em geral por meio de bitcoins.

As afirmativas apresentam características, de cima para baixo, correspondentes a

a) Spyware – Keylogger – Trojan
b) Spyware – Printscreen – Spyware
c) Adware – Keylogger – Ransomware
d) Adware – Screenlogger – Wormware
e) Worm – Printlog – Warmware

020. (Q2729813/FEPESE/PREF. ÁGUAS DE CHAPECÓ/AGENTE DE RECURSOS HUMANOS/2023) No âmbito da segurança, assinale a alternativa que define corretamente ransomware.

a) É um ataque de força bruta que busca exaurir as possibilidades de combinações de modo a deduzir a senha do usuário e obter acesso à sua conta.
b) É um software malicioso que se instala no computador silenciosamente e monitora todas as ações de entrada de dados, via teclado e também via mouse.
c) É um ataque de engenharia social que consiste em ganhar a confiança do usuário para que este forneça voluntariamente dados pessoais e credenciais.
d) É um ataque que consiste em criptografar dados do usuário e solicitar um resgate para fornecer a chave que torna os dados acessíveis novamente.
e) É uma técnica de monitoramento de tráfego de rede que escuta os dados que passam no cabo ou wireless e os captura.

021. (Q2862805/QUADRIX/CRO-MS/ANALISTA ADMINISTRATIVO/2023) Em relação aos conceitos de organização e de gerenciamento de arquivos e de programas, aos procedimentos de segurança da informação e às noções de vírus, worms e pragas virtuais, julgue os itens.
O ransomware, programa similar ao worm, apresenta mecanismos de comunicação com o invasor, os quais permitem que aquele seja remotamente controlado. A principal característica desse programa é a capacidade de se propagar automaticamente pelas redes, com o envio de cópias de si mesmo de um equipamento para outro.

022. (Q2805091/SELECON/PREF. NOVA MUTUM/INSTRUTOR DE INFORMÁTICA/2023) Um ambiente de rede de computadores sofreu um ataque de um hacker, que consistiu no recebimento de mensagens com endereços IP de origem falsos, de modo que o sistema para o qual o pacote foi direcionado não conseguisse identificar corretamente o remetente. Esse tipo de ataque também é conhecido como:
a) SYN Flood
b) Brute Force
c) IP Spoofing
d) Session Hijack

023. (Q2878245/QUADRIX/CAU-TO/AGENTE DE FISCALIZAÇÃO/2023) No que diz respeito aos conceitos de organização e de gerenciamento de arquivos e de pastas, aos sítios de busca e de pesquisa na Internet e às noções de vírus, worms e pragas virtuais, julgue os itens.
Com a finalidade de monitorar computadores e dispositivos, um adware pode atuar como um spyware.

024. (Q2676498/IF-MT/TÉCNICO DE LABORATÓRIO/ÁREA: INFORMÁTICA/2023) Leia as sentenças abaixo.

I. programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento.
II. conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um equipamento comprometido.
III. programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
IV. programa que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado.
As sentenças dizem respeito a códigos maliciosos e são, respectivamente, as definições de:
a) Vírus, Worm, Bot e Rootkit
b) Botnet, Ramsonware, Trojan e Worm
c) Rootkit, Vírus, Trojan e Botnet
d) Worm, Rootkit, Backdoor e Bot
e) Trojan, Worm, Vírus e Rootkit

025. (Q2674596/IADES/SEAGRI-DF/TÉCNICO DE DESENVOLVIMENTO AGROPECUÁRIA/ÁREA AGENTE ADMINISTRATIVO/2023) Uma modalidade comum de ataques cibernéticos se utiliza de programas para edição de texto, planilhas ou apresentações para incluir código malicioso e autorreplicável em rotinas pré-definidas que são incorporadas aos documentos manipulados por esses aplicativos. Essa modalidade de ataque denomina-se
a) vírus de macro
b) SQL injection
c) exploit
d) cavalo de Troia
e) middleware

026. (Q2735119/FUNDEP/PREF. LAVRAS/AGENTE DE TRÂNSITO/2023) O tipo de spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento é chamado de
a) Keylogger.
b) Worm.
c) Backdoor.
d) Cavalo de Troia.

027. (Q2703129/FUNDAÇÃO CEFETMINAS/IFB/PROFESSOR/ÁREA: EDIÇÃO/VIDEOGRAFISMO/2023) Qual a descrição do ataque denominado “força bruta”?

a) O atacante sobrecarrega o sistema com inúmeras requisições, forçando o servidor tornar o sistema indisponível.
b) O atacante tenta acesso ao sistema através de tentativa e erro, utilizando como base uma lista de nomes de usuários e senhas aleatórias.
c) Um grupo de atacantes utiliza diversos computadores infectados na internet para que, através de um ataque em massa, ocasione uma indisponibilidade no sistema e a partir de então seja possível assumir o controle.
d) O atacante envia um arquivo para o computador da vítima e, ao ser aberto, o arquivo criptografa todo o sistema da vítima. Por fim, o atacante solicita dinheiro em troca da chave para descriptografar os arquivos.
e) O atacante envia um link malicioso pelo e-mail da vítima. Ao abrir o link, o computador da vítima é bloqueado de maneira forçada.

028. (Q2700119/IBADE/FUNDAÇÃO FACELI/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2023) _____ é um ataque que tenta roubar seu dinheiro ou a sua identidade fazendo com que você revele informações pessoais, tais como: números de cartão de crédito, informações bancárias ou senhas em sites que fingem ser legítimos. Assinale a alternativa que preencha a lacuna acima.
a) Pharming
b) Phishing
c) Rootkits
d) Keyloggers
e) Adware

029. (Q2849791/FUNDEP/CRO-MG/CONTADOR/2023) O código malicioso que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o consentimento do usuário é chamado de
a) Spyware.
b) Cavalo de Troia.
c) Rootkit.
d) Spam.

030. (Q2729926/INQC/COMDEP/ASSISTENTE ADMINISTRATIVO/2023) No caso de um usuário de computador estar diante de um ataque, no qual o atacante cria uma aparência de que as comunicações oriundas dele vêm de uma fonte confiável, diz-se que o usuário sofreu um ataque denominado:

a) dialer
b) synflood
c) spoofing
d) keylogger

031. (Q4284426/QUADRIX/SES-SP/TÉCNICO DE ENFERMAGEM/2026) Um malware infectou um computador da rede hospitalar e, diferentemente de um vírus comum que precisa ser executado pelo usuário (clicando em um arquivo), este programa malicioso começou a se replicar automaticamente através das falhas de segurança da rede, infectando dezenas de outras máquinas conectadas em questão de minutos, sem nenhuma intervenção humana. Com base nessa situação hipotética, assinale a opção que apresenta a classificação específica dessa praga virtual que se propaga autonomamente pela rede.
a) trojan
b) ransomware
c) adware
d) worm
e) keylogger

032. (Q4296858/INSTITUTO AOCP/SEJUSP-MG/POLICIAL PENAL/2026) Durante o turno vespertino na sala de controle de acesso de uma unidade prisional, o policial penal recebe diversas notificações sobre acessos irregulares ao sistema interno e tentativas de login feitas com credenciais de servidores que não estavam de plantão. Após verificação, constata-se que todos os usuários afetados haviam utilizado o mesmo computador recentemente. Não há evidências de e-mails fraudulentos nem de arquivos criptografados, e o terminal aparentemente funciona de forma normal. Considerando as principais ameaças digitais e seus modos de atuação, é correto afirmar que o incidente descrito retrata a ameaça de um
a) keylogger, programa espião que registra silenciosamente todas as teclas digitadas, capturando logins e senhas inseridos no terminal para posterior envio ao invasor.
b) phishing, golpe eletrônico que simula comunicações legítimas e induz o usuário a informar suas credenciais em um site falsificado.
c) ransomware, software malicioso que criptografa os dados do sistema e exige pagamento para liberar o acesso aos arquivos.
d) sniffer, ferramenta usada para interceptar pacotes de dados na rede local, capturando informações transmitidas sem criptografia.

033. (Q4299042/FGV/AMAZUL/ESPECIALISTA DE RADIOPROTEÇÃO/2026) No contexto de segurança da informação, mais especificamente sobre malwares, associe corretamente o cada item numerado no primeiro bloco (variando de 1 a 4) às lacunas do segundo bloco.

1. Cavalo de Troia (trojan horse) **2**. Verme (worm) **3**. Bomba lógica (logic bomb) **4**. Zumbi (zumbi, bot)	( ) Execução autônoma com capacidade de replicação automática e propagação entre sistemas conectados. ( ) Malware ativado por condição predefinida após período hibernado. ( ) Ataque a outras máquinas executado por software malicioso instalado em host comprometido. ( ) Software aparentemente útil que possui desvio oculto e malicioso de finalidade.

Assinale a opção que corretamente associa o nome do malware no primeiro bloco e a característica apresentada no segundo bloco.
a) 1 – 2 – 4 – 3
b) 4 – 1 – 3 – 2
c) 2 – 3 – 4 – 1
d) 1 – 3 – 2 – 4
e) 3 – 4 – 2 – 1

034. (Q4272276/QUADRIX/CRQ 7/ASSISTENTE ADMINISTRATIVO/2026) Em relação aos conceitos de redes de computadores, às noções de vírus, worms e pragas virtuais e aos conceitos de inteligência artificial (IA), julgue os itens seguintes.
O ransomware é uma praga virtual que tem como principal característica capturar dados pessoais do usuário e utilizá-los para enviar spam sem solicitar permissão.

035. (Q4386081/QUADRIX/CRF-DF/ADMINISTRADOR/2026) Acerca de redes de computadores, antivírus e computação em nuvem, julgue os itens a seguir.
Todo malware que executa código automaticamente sem intervenção do usuário é classificado como vírus.

036. (Q4383739/CEBRASPE-CESPE/Câmara dos Deputados/Analista Legislativo/Área: Processo Legislativo e Gestão/2026)Julgue os itens seguintes, relativos a procedimentos de backup, vírus e worms, soluções anti-spyware e ameaças pharming.
O pharming caracteriza-se pela manipulação direta do conteúdo apresentado ao usuário no navegador por meio de código malicioso, com atuação associada à modificação dinâmica de páginas durante a sessão.

037. (Q4328132/FGV/ALE-GO/POLICIAL LEGISLATIVO/2026) Durante uma busca na internet por informações sobre um edital de licitação, um Assessor Legislativo da ALE-GO acessou um site de notícias. Na lateral da página, um anúncio chamativo dizia:

SEU COMPUTADOR PODE ESTAR INFECTADO! CLIQUE AQUI PARA VERIFICAR AGORA!
O Assessor Legislativo percebeu que o site principal era confiável, mas desconfiou desse anúncio específico. A sua desconfiança é fundamentada no fato de que esse tipo de anúncio é comumente associado a uma prática maliciosa específica que é conhecida como
a) Phishing
b) Spam
c) Ransomware
d) Backdoor
e) Scareware

038. (Q4284410/QUADRIX/SES-SP/FISIOTERAPEUTA/2026) Todos os funcionários do hospital receberam um e-mail com o logotipo do banco que processa a folha de pagamento, informando: "Seus dados cadastrais estão desatualizados e seu salário será bloqueado. Clique AQUI para atualizar imediatamente". O link direcionava para um site falso, visualmente idêntico ao do banco, projetado para roubar a senha do usuário.Com base nessa situação hipotética, assinale a opção que apresenta o nome técnico desse tipo de fraude com base em engenharia social.
a) DDoS
b) phishing
c) hoax
d) furto de identidade
e) brute force

039. (Q4299458/FGV/AMAZUL/TÉCNICO DE INFORMÁTICA/2026) O uso de programas maliciosos (malwares) em crimes cibernéticos é cada vez mais associado a objetivos bem específicos, como espionagem, fraude financeira, controle remoto de máquinas e fraudes correlatas. Considerando os diferentes tipos de malware e seus objetivos principais, assinale a opção que corretamente indica o nome do malware que tem como propósito sequestrar a máquina e exigir, por extorsão, o pagamento de resgate.
a) Backdoor
b) Banking Trojans
c) Bots
d) Malware APT
e) Ransomware

040. (Q4299526/FGV/AMAZUL/TÉCNICO DE INFORMÁTICA/2026) Durante um incidente, a equipe detecta um programa que se replica automaticamente explorando falhas em serviços de rede internos. O tipo de malware descrito por esse comportamento é

a) Worm
b) Vírus
c) Cavalo de Troia
d) Spyware
e) Backdoor

041. (Q3779541/QUADRIX/CRF-MS/ASSISTENTE ADMINISTRATIVO/2025) Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.
Um vírus de computador é um(a)
a) programa malicioso que se replica, anexando-se a arquivos executáveis e depende da ação do usuário para se espalhar.
b) componente do sistema operacional que impede a instalação de softwares não autorizados.
c) programa autônomo que se espalha automaticamente pela rede, sem intervenção do usuário.
d) ferramenta de segurança que monitora e corrige falhas do sistema.
e) um arquivo de dados sensíveis e ilegais.

042. (Q4138304/QUADRIX/CORE-SE/CONTADOR/2025) Um usuário percebeu que a tela do seu computador estava abrindo diversos anúncios em janelas “pop-ups”, mesmo quando não estava navegando em sites suspeitos. Além disso, o navegador teve sua página inicial e seu mecanismo de busca alterados sem sua permissão. Com base nessa situação hipotética e considerando os vírus, worms e outras pragas virtuais, assinale a opção que apresenta o tipo de malware que causa esse comportamento.
a) ransomware
b) adware
c) keylogger
d) worm
e) rootkit

043. (Q4061424/QUADRIX/CRO-SP/AUXILIAR ADMINISTRATIVO/2025) Quanto ao uso de webmails, ao armazenamento em nuvem e às noções de vírus, worms e pragas virtuais, julgue os itens seguintes.
Um spyware, diferentemente de um vírus, tem como objetivo principal a replicação automática e o comprometimento de arquivos do sistema operacional.

044. (Q4132847/CEBRASPE-CESPE/TCE-RS/OFICIAL DE CONTROLE EXTERNO/ÁREA: OFICIAL INSTRUTIVO/2025) No que se refere a armazenamento de dados na nuvem, pragas virtuais e firewall, julgue os itens subsequentes.
Spyware é um programa que se replica ao infectar arquivos ou documentos que contenham código executável.

045. (Q4288713/INSTITUTO AOCP/UENF/TÉCNICO EM NÍVEL SUPERIOR/ÁREA: BIBLIOTECA/2025) A segurança na internet envolve uma série de práticas e tecnologias que visam proteger usuários, dispositivos e dados durante o uso de redes digitais, com o objetivo de prevenir fraudes, invasões e roubos de informações. Dentro desse contexto, há diversas ameaças e técnicas usadas para comprometer a segurança. Sabendo disso, assinale a alternativa que descreve uma técnica de manipulação psicológica voltada para enganar usuários e obter dados confidenciais, como senhas ou informações bancárias.
a) Spoofing
b) Criptografia
c) Rootkit
d) Certificado digital
e) Engenharia social

046. (Q4377334/INSTITUTO AOCP/IF-PB/TÉCNICO EM ASSUNTOS EDUCACIONAIS/2025) O malware conhecido como Cavalo de Troia (Trojan) é amplamente utilizado por atacantes. Sua característica definidora não é o método de replicação, mas sim a sua forma de distribuição e execução inicial. O Cavalo de Troia se distingue dos Vírus e Worms
a) pela sua capacidade de se replicar automaticamente pela rede, explorando vulnerabilidades sem a interação do usuário.
b) porque sua principal ação é criptografar arquivos do sistema operacional para exigir um pagamento de resgate.
c) porque, no Trojan, o código malicioso se anexa a arquivos executáveis legítimos e se espalha junto com eles.
d) porque ele se disfarça de programa legítimo e, dessa forma, é útil para enganar o usuário a instalá-lo voluntariamente, criando uma porta de acesso.
e) porque ele opera no nível de kernel do sistema operacional para ocultar a presença de outros softwares maliciosos.

047. (Q3979898/CEBRASPE-CESPE/CAESB/OPERADOR DE ESTAÇÃO DE TRATAMENTO/2025) Certo dia, Paulo recebeu um email que pensou ter sido enviado pelo banco. Ele foi informado que sua conta tinha sido comprometida e que seria necessário clicar no link fornecido para bloquear o acesso das informações pessoais a terceiros de má-fé. Ao clicar, Paulo

foi direcionado a um site falso, idêntico ao do banco, e inseriu os dados que criminosos cibernéticos precisavam para que tivessem acesso à conta. Considerando as informações na situação hipotética precedente, assinale a opção que corresponde ao tipo de golpe digital aplicado em Paulo.
a) phishing
b) spyware
c) ransomware
d) vírus
e) trojan

048. (Q3765330/CEBRASPE-CESPE/AEB/TECNOLOGISTA JÚNIOR/ÁREA: TECNOLOGIA DA INFORMAÇÃO/2025) Um malware projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros é do tipo
a) trojan
b) ransoware
c) adware
d) rootkit
e) spyware

049. (Q3938162/IADES/CRMV-PI/TÉCNICO ADMINISTRATIVO/2025) Uma prática maliciosa comum na internet consiste no envio de e-mails fraudulentos que tentam se passar por comunicações de empresas ou instituições conhecidas para enganar o usuário e induzi-lo a fornecer dados pessoais e senhas. Esse tipo de golpe é conhecido como
a) adware.
b) spam.
c) firewall.
d) phishing.
e) spyware.

050. (Q3915018/CEBRASPE-CESPE/FUB/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2025) Em relação a vírus e antivírus, julgue os itens seguintes.
Rootkit é um tipo de vírus que liberam acesso ao computador para softwares não autorizados.

GABARITO

1. d
2. E
3. C
4. e
5. c
6. C
7. d
8. a
9. c
10. e
11. E
12. a
13. E
14. a
15. d
16. E
17. b
18. C
19. c
20. d
21. E
22. c
23. C
24. d
25. a
26. a
27. b
28. b
29. b
30. c
31. d
32. a
33. c
34. E
35. E
36. E
37. e
38. b
39. e
40. a
41. a
42. b
43. E
44. E
45. e
46. d
47. a
48. e
49. d
50. E

GABARITO COMENTADO

001. (Q2681739/FEPESE/PREF. PINHALZINHO/PROF. INFORMÁTICA/2023/ADAPTADA) As tentativas ofensivas dos hackers de penetrar em redes e sistemas a fim de causar danos ou roubar dados são chamadas de ameaças virtuais. Assinale a alternativa que descreve corretamente o tipo de ameaça e sua definição.

a) O Ransomware é um programa que permite que uma pessoa controle um computador infectado a distância.

b) O Kidnapper é um programa que sequestra os arquivos e dados de um usuário, com a ameaça de apagá-los, a menos que um resgate seja pago.

c) O Cavalo de Troia (Trojan) é um programa que recolhe informações sobre o usuário e transmite essa informação a uma entidade externa. Pode ser usado para roubar dados bancários, por exemplo.

d) O vírus é um programa que se prende a um arquivo limpo. A partir disso, ele se espalha pelo sistema de computadores, infectando arquivos com algum código malicioso.

e) O worm (verme) é um programa de computador autorreplicante que infecta um programa para se propagar; além disso, pode ser projetado para tomar ações maliciosas tais como deletar um arquivo ou mandar um email.

a) Conceito de **Bot**: é um programa que permite que uma pessoa controle um computador infectado a distância.

b) Conceito de **Ransomware**: é um programa que sequestra os arquivos e dados de um usuário, com a ameaça de apagá-los, a menos que um resgate seja pago.

c) **Cavalo de Troia**: atua como um transporte para essas ameaças se infiltrarem em um sistema.

d) Nosso gabarito: **vírus** é um código malicioso executável. Eles são desenvolvidos por programadores de software e são inseridos em algum outro arquivo executável de algum programa ou em documentos, como os do Word ou Excel. Com isso, ele se espalha pelo sistema operacional do computador, infectando arquivos com uma cópia do seu código.

e) **Worm**: não infecta programas ou arquivos; a finalidade dele é causar a indisponibilidade do serviço por meio da exploração de vulnerabilidades.

Letra d.

---

002. (Q2733022/QUADRIX/CREF 3/JORNALISTA/2023) Julgue os itens, relativos aos conceitos de organização e de gerenciamento de arquivos, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup.

Os vírus não são considerados programas maliciosos, pois são criados pelos crackers, e não pelos hackers.

Em informática, vírus é um software desenvolvido por programadores, hackers ou crackers mal-intencionados com o objetivo de perturbar as atividades no ambiente computacional.
Errado.

---

003. (Q2733017/QUADRIX/CREF 3/ANALISTA TI/2023 (FACIL))Julgue os itens, relativos aos conceitos de organização e de gerenciamento de arquivos, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup.
Códigos maliciosos podem executar ações danosas e atividades maliciosas em equipamentos como roteadores.

Malware é todo tipo de código malicioso que tem uma intenção danosa por trás, seja apagar arquivos, comprometer o funcionamento do micro, desconfigurar o sistema operacional, desinstalar dispositivos de hardware ou realizar fraudes bancárias, entre vários outros males que possam causar.
Certo.

---

004. (Q2732571/OBJETIVA CONCURSOS/PREF. SAGRADA FAMÍLIA/MONITOR DE ENSINO/2023) Adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome desse usuário e com os mesmos privilégios dele é uma clássica técnica utilizada por indivíduos mal-intencionados. Essa técnica é popularmente conhecida como:
a) Scan
b) Spoofing
c) Sniffing
d) Malware
e) Brute force

a) **Scan** é uma técnica de varredura que consiste em identificar hosts ativos (computadores ativos) e possíveis vulnerabilidades no sistema, possibilitando um ataque à vítima.
b) **Spoofing** é um crime cibernético em que o atacante tenta se passar por uma pessoa conhecida dos contatos ou por instituições reconhecidas, com a finalidade de ganhar a confiança do usuário. O objetivo desse ataque consiste em obter acesso às informações e contornar medidas de segurança.

c) Sniffing é uma técnica utilizada por atacantes com o objetivo de capturar, por exemplo, senhas, números de cartão de crédito e conteúdos confidenciais que estejam trafegando sem criptografia nas redes.
d) **Malware** é todo tipo de código malicioso que tenha uma intenção danosa por trás, seja apagar arquivos, comprometer o funcionamento do micro, desconfigurar o sistema operacional, desinstalar dispositivos de hardware, realizar fraudes bancárias, entre vários outros males que possam causar.
e) **Brute Force** (**Força Bruta**) é um ataque cibernético que consiste em adivinhar o login (nome de usuário) e a senha do usuário por tentativa e erro. O objetivo do atacante é possuir os mesmos privilégios de acesso do usuário/vítima.
Letra e.

---

005. (Q2828627/GUALIMP/PREF. BOM JARDIM/PROFESSOR II/ÁREA HISTÓRIA/2023) Existe uma prática ilícita onde usuários de internet são levados a revelarem informações pessoais, como senhas de cartão de crédito ou informações bancárias, ao acessarem sites que parecem legítimos. Essa prática é chamada de:
a) Extorsão.
b) Ransomware.
c) Phishing.
d) Trojan.

a) **Extorsão** não é um tipo de código malicioso.
b) **Ransomware** é um tipo de malware que sequestra os dados e cobra um valor pelo resgate (ransom), daí a origem do seu nome.
c) **Phishing** é um tipo de golpe em que o golpista tem o objetivo de obter os dados pessoais e financeiros da vítima; para isso, ele combina o uso de tecnologia com engenharia social.
d) **Cavalo de Troia** é um tipo de malware que se disfarça como um presente ou aplicativo útil, mas traz consigo várias ameaças, como vírus, worms, bots e spywares.
Letra c.

---

006. (Q2825373/QUADRIX/CREFONO 2/ASSISTENTE DE COMPRAS/2023) Acerca do programa de correio eletrônico Microsoft Outlook, versão web, dos conceitos de organização e de gerenciamento de programas, bem como das noções de vírus, de worms e de pragas virtuais, julgue os itens.
O phishing é uma técnica de engenharia social em que os criminosos se passam por empresas ou por pessoas confiáveis para a obtenção de informações pessoais ou financeiras das vítimas.

O phishing é um tipo de golpe em que o golpista tem o objetivo de obter os dados pessoais e financeiros da vítima. Para isso, ele combina o uso de tecnologia com engenharia social.
Certo.

---

007. (Q2706739/FUNDEP/PREF. BARRA LONGA/ASSISTENTE SOCIAL/CRAS/2023) Um Trojan, também conhecido como Cavalo de Troia, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas. Um Trojan pode ser obtido das seguintes maneiras, exceto:
a) A partir de um e-mail.
b) Por meio de compartilhamento de arquivos.
c) Por meio de mensagens instantâneas.
d) De forma automática pela rede.

Esse tipo de malware pode chegar ao usuário como programas, arquivos anexados em e-mails, atualizações fraudulentas, downloads de fontes não confiáveis, mensagens instantâneas, entre outros. O Trojan não pode chegar de maneira automática pela rede.
Letra d.

---

008. (Q2693421/OBJETIVA CONCURSOS/PREF. SÃO JOSÉ DO INHACORÁ/AGENTE EDUCACIONAL/2023) Phishing, phishing-scam ou phishing/scam é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social. Com relação ao phishing, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

( ) O phishing geralmente ocorre por meio do envio de mensagens eletrônicas.
( ) O fraudador tenta se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular.
( ) Uma das formas de prevenção contra esse tipo de fraude é utilizar mecanismos de segurança, como programas antimalware, firewall pessoal e filtros antiphishing.

a) C – C – C
b) E – E – C
c) C – E – E
d) E – C – C

O phishing é um tipo de golpe em que o golpista tem o objetivo de obter os dados pessoais e financeiros da vítima; para isso, ele combina o uso de tecnologia com engenharia social. Esse golpe é realizado por meio do envio de mensagens eletrônicas que se passam por instituições conhecidas, como bancos, sites populares ou empresas. Ao utilizar ferramentas como antimalware, firewall pessoal e filtros antiphishing, o usuário minimiza a chegada de ameaças e o acesso a sites fraudulentos.

Letra a.

---

009. (Q2720449/FUNDEP/PREF. URUCÂNIA/AUXILIAR ADMINISTRATIVO/2023) Hoje em dia, há vários ataques a informações na internet. Conforme o cert.br, a técnica que consiste em efetuar buscas minuciosas nas redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles, é chamada de

a) Sniffing.
b) Brute force.
c) Scan.
d) DDoS.

a) **Sniffing** é uma técnica utilizada por atacantes com o objetivo de capturar, por exemplo, senhas, números de cartão de crédito e conteúdos confidenciais que estejam trafegando sem criptografia nas redes.

b) **Brute Force** (**Força Bruta**) é um ataque cibernético que consiste em adivinhar o login (nome de usuário) e a senha do usuário por tentativa e erro. O objetivo do atacante é possuir os mesmos privilégios de acesso do usuário/vítima.

c) **Scan** é uma técnica de varredura que consiste em identificar hosts ativos (computadores ativos) e possíveis vulnerabilidades no sistema, possibilitando um ataque à vítima.

d) **DDoS** é a negação de serviço distribuída, um ataque feito em massa, atingindo centenas de servidores e sites da internet, tirando-os de funcionamento.

Letra c.

---

010. (Q2687166/FUNDAÇÃO CEFETMINAS/PREF. CONTAGEM/AGENTE FAZENDÁRIO/2023) O programa malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário é denominado

a) Spam
b) Adware

c) Keylogger
d) Screenlogger
e) Ransomware

a) **Spam** é a mensagem eletrônica NÃO SOLICITADA, geralmente enviada para um grande número de pessoas.
b) **Adware** é um tipo de spyware projetado para parecer uma propaganda.
c) **Keylogger** é um spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador.
d) **Screenlogger** captura prints da tela quando o mouse é clicado, permitindo que o atacante tenha acesso aos dados contidos na tela printada.
e) **Ransomware** é um tipo de malware que sequestra os dados e cobra um valor pelo resgate (ransom), daí a origem do seu nome.
Letra e.

---

011. (Q2866736/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA: TÉCNICO ADMINISTRATIVO/2023 (FACIL))No que diz respeito ao programa de navegação Mozilla Firefox, em sua versão mais atual, aos procedimentos de segurança da informação e às noções de vírus, worms e pragas virtuais, julgue os itens.
Os vírus de computador não representam uma ameaça à segurança da informação, uma vez que a finalidade deles é apenas o comprometimento do desempenho do computador.

Essa questão está errada, pois vírus é uma ameaça com distintas finalidades maliciosas, nas quais os atacantes têm o objetivo de perturbar as atividades no ambiente computacional, como corromper arquivos, desinstalar programas e desconfigurar o sistema operacional.
Errado.

---

012. (Q2723361/GUALIMP/PREF. DIVINO/ASSISTENTE ADMINISTRATIVO/2023) "Quem navega bastante pela Internet costuma fazer compras em lojas virtuais e, atraído pela promessa de descontos, acaba baixando o Jollywallet. [...] Jollywallet exibe anúncios no computador do usuário e se conecta à web em segundo plano. Criado pela Media Radyoos, o aplicativo é instalado como um add-on (complemento/extensão) para navegadores e também aplica um botão ao lado da caixa de endereços, para acessá-lo rapidamente."

(Fonte: https://www.techtudo.com.br/noticias/2014/02/como-remover-o-jollywallet-do-computador.ghtml).

Pela descrição acima, o Jollywallet é classificado como um:

a) Adware
b) Trojan
c) Ransomware
d) Worm

a) **Adware** é um tipo de spyware projetado para parecer uma propaganda e está relacionado a anúncios.
b) **Cavalo de Troia** digital é um tipo de malware que se disfarça como um presente ou aplicativo útil, mas traz consigo várias ameaças, como vírus, worms, bots e spywares.
c) **Ransomware** é um tipo de malware que sequestra os dados e cobra um valor pelo resgate (ransom), daí a origem do seu nome.
d) **Worm** é um malware especializado em explorar vulnerabilidades e tem como objetivo causar negação de serviço.
Letra a.

---

013. (Q2731752/QUADRIX/CRESS AL/ASSISTENTE TÉCNICO ADMINISTRATIVO/2023) Quanto aos conceitos de organização e de gerenciamento de arquivos, pastas e programas, aos procedimentos de segurança da informação e aos procedimentos de backup, julgue os itens.
A engenharia social é o ataque mais difícil de ser identificado, logo não há como preveni-lo.

A engenharia social é um método de ataque que utiliza a persuasão para a obtenção dos dados sigilosos do usuário. Esse ataque explora as vulnerabilidades humanas por meio de manipulação e convencimento. Contudo, não é o ataque mais difícil de ser identificado, visto que há frequente divulgação de orientações e alertas sobre esse tipo de ameaça.
Errado.

---

014. (Q2791834/FUNDAÇÃO CEFETMINAS/IFSULDEMINAS/MÉDICO/ÁREA CLÍNICA GERAL/2023) Qual é o tipo de fraude de internet por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social, via mensagens eletrônicas?
a) Phishing
b) Advance fee fraud
c) Identity theft
d) Fake news
e) Spyware

a) **Phishing** é um tipo de golpe em que o golpista tem o objetivo de conseguir obter os dados pessoais e financeiros da vítima; para isso, ele combina o uso de tecnologia associado à engenharia social.
Esse golpe é realizado por meio do envio de mensagens eletrônicas que se passam por instituições conhecidas, como bancos, sites populares ou empresas.
b) **Advance fee fraud** ou golpe de taxa antecipada é um tipo de fraude em que um golpista tenta enganar a vítima a pagar uma taxa adiantada em troca de algo que não existe ou que não vale o dinheiro. O golpista pode usar uma variedade de técnicas para enganar a vítima, como e-mail de phishing, chamadas telefônicas ou até mesmo pessoalmente.
c) **Identity theft** é um ataque no qual ocorre o roubo da identidade do usuário e o atacante se passa pelo usuário perante os sistemas computacionais.
d) **Fake News** são notícias falsas propagadas principalmente por redes sociais, sites não confiáveis e aplicativos de mensagens como Telegram e WhatsApp, com a finalidade de manipular e/ou enganar pessoas.
e) **Spyware** é uma categoria de malware que atua como um espião, coletando dados do usuário sem seu conhecimento ou consentimento. Esses tipos de malware são classificados como spywares devido ao seu propósito de capturar informações pessoais sem o conhecimento do usuário.
Letra a.

---

015. (Q2824947/INSTITUTO AOCP/PM-DF/2º TENENTE/ÁREA: ADMINISTRAÇÃO/2023) Considerando o comportamento de softwares maliciosos, um BOT é um programa similar a um WORM. A característica específica que diferencia um BOT de um WORM é o fato de o
a) BOT oferecer recursos de captura de teclas digitadas em um teclado virtual.
b) BOT ser projetado para monitorar as atividades em um computador e enviar as informações coletadas para o invasor.
c) BOT ser um programa que torna indisponíveis os dados em um computador, a fim de exigir pagamento de resgate para a restauração do acesso para o usuário.
d) BOT possuir recursos de comunicação com o invasor que permite que o computador infectado seja remotamente controlado.
e) BOT poder ser utilizado por um invasor para apresentar propagandas na tela do usuário, a fim de gerar monetização a partir do acesso às propagandas.

O termo bot é utilizado para descrever uma evolução do worm, que é aprimorado com mecanismos de conexão que permitem ao atacante se conectar ao malware e enviar comandos remotos.
Letra d.

---

016. (Q2822437/QUADRIX/CRO-PB/AGENTE ADMINISTRATIVO/2023) No que se refere ao programa de navegação Mozilla Firefox, em sua versão mais recente, ao programa de correio eletrônico Microsoft Outlook e às noções de vírus de computador, julgue os itens.
Os vírus de computador não possuem capacidade para tornar o sistema operacional inoperante.

Em informática, vírus é um software desenvolvido por programadores mal-intencionados com o objetivo de perturbar as atividades no ambiente computacional, podendo tornar o sistema operacional inoperante. Um exemplo de vírus que torna o sistema operacional inoperante é o vírus de boot, o qual corrompe os arquivos de inicialização do sistema operacional, impedindo-o de ser inicializado.
Errado.

---

017. (Q2672798/INSTITUTO AVALIA/PREF. SANT'ANA DO LIVRAMENTO/ANALISTA JUDICIÁRIO/2023) Assinale a alternativa que apresenta um tipo de malware que parece ser um programa inofensivo, porém, quando ativado, realiza a abertura de backdoors.
a) Rootkit
b) Cavalo de Troia
c) Bombas-relógio
d) Vírus
e) Spywares

a) **Rootkit** refere-se a um conjunto de programas e técnicas realizadas para esconder e assegurar a permanência do atacante ou até mesmo de outro código malicioso no computador infectado da vítima. Então, se disfarçam como um utilitário ou software de manutenção ou gerenciamento, com o objetivo de obter privilégios de administrador (root).
b) **Cavalo de Troia** é um tipo de malware que se disfarça como um presente ou aplicativo útil; parece inofensivo, mas traz consigo várias ameaças, como vírus, worms, bots, backdoors e spywares.
c) **Vírus bomba-relógio** é projetado para causar danos no ambiente digital no momento de sua ativação. Ao ser ativado, pode executar ações como apagar arquivos, corromper dados e causar danos ao sistema operacional, entre outros. A finalidade desse malware é causar prejuízos ao
d) **Vírus** é um código malicioso executável. Eles são desenvolvidos por programadores de software e são inseridos em algum outro arquivo executável de algum programa ou em documentos, como os do Word ou Excel. Com isso, ele se espalha pelo sistema operacional do computador, infectando arquivos com uma cópia do seu código.

e) **Spyware** é uma categoria de malware que atua como um espião, coletando dados do usuário sem seu conhecimento ou consentimento. Esses tipos de malware são classificados como spywares devido ao seu propósito de capturar informações pessoais sem o conhecimento do usuário.

Letra b.

---

018. (Q2684981/QUADRIX/CRO/AGENTE FISCAL/2023) Considerando o programa de navegação Mozilla Firefox, sítios de busca na Internet e noções de malwares e outras pragas virtuais, julgue os itens de 34 a 37.

Os ataques de malvertising acontecem quando cibercriminosos introduzem anúncios malignos em redes de publicidade online.

O ataque de Malvertising está relacionado à inserção de anúncios maliciosos de propaganda em sites de publicidade legítimos. Para que isso ocorra, os golpistas criam anúncios fraudulentos ou maliciosos e os distribuem como se fossem anúncios legítimos em sites de publicidade, que dão visibilidade em diversos sites da web.

Certo.

---

019. (Q2793774/COTEC/FADENOR/PREF. FRANCISCO SÁ/ANALISTA FAZENDÁRIO/2023) Considere as seguintes características aplicáveis a malwares:

I – Projetado especificamente para apresentar propagandas, ele pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro, e para fins maliciosos, quando as propagandas apresentadas são redirecionadas sem conhecimento do usuário.

II – Capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador, a sua ativação, em muitos casos, está condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking, por exemplo.

III – Tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, ele exige pagamento de resgate para restabelecer o acesso ao usuário, em geral por meio de bitcoins.

As afirmativas apresentam características, de cima para baixo, correspondentes a

a) Spyware – Keylogger – Trojan

b) Spyware – Printscreen – Spyware

c) Adware – Keylogger – Ransomware

d) Adware – Screenlogger – Wormware

e) Worm – Printlog – Warmware

I – **Adware** – projetado especificamente para exibir anúncios. Ele pode ser usado para fins legítimos, como uma forma de patrocínio ou retorno financeiro, ou para fins maliciosos, como uma forma de rastrear os hábitos de navegação do usuário ou roubar informações pessoais. Adware legítimo geralmente é incluído em programas e serviços com o consentimento do usuário. O adware pode ser usado para gerar receita para os desenvolvedores do programa ou serviço, ou pode ser usado para promover produtos ou serviços relacionados. Por exemplo, um navegador da web pode incluir adware que exibe anúncios para produtos que são relevantes para os interesses do usuário. Adware malicioso, por outro lado, é instalado no computador do usuário sem o seu consentimento. O adware malicioso pode ser usado para rastrear os hábitos de navegação do usuário, roubar informações pessoais ou até mesmo instalar outros malwares. Por exemplo, um programa de adware malicioso pode exibir anúncios que redirecionam o usuário para sites maliciosos ou pode roubar as informações de cartão de crédito do usuário.
II – **Keylogger** – é um tipo de malware que é capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. A ativação do keylogger, em muitos casos, está condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking, por exemplo. Ao capturar as teclas digitadas, o keylogger pode roubar informações pessoais do usuário, como senhas, números de cartão de crédito e números de contas bancárias. Essas informações podem ser usadas para cometer fraudes financeiras, como roubo de identidade e compras não autorizadas.
III – **Ransomware** – tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia; ele exige pagamento de resgate para restabelecer o acesso ao usuário, em geral por meio de bitcoins.
Letra c.

---

020. (Q2729813/FEPESE/PREF. ÁGUAS DE CHAPECÓ/AGENTE DE RECURSOS HUMANOS/2023) No âmbito da segurança, assinale a alternativa que define corretamente ransomware.
a) É um ataque de força bruta que busca exaurir as possibilidades de combinações de modo a deduzir a senha do usuário e obter acesso à sua conta.
b) É um software malicioso que se instala no computador silenciosamente e monitora todas as ações de entrada de dados, via teclado e também via mouse.
c) É um ataque de engenharia social que consiste em ganhar a confiança do usuário para que este forneça voluntariamente dados pessoais e credenciais.
d) É um ataque que consiste em criptografar dados do usuário e solicitar um resgate para fornecer a chave que torna os dados acessíveis novamente.
e) É uma técnica de monitoramento de tráfego de rede que escuta os dados que passam no cabo ou wireless e os captura.

a) Conceito do ataque de força bruta.
b) Conceito de keylogger.
c) Conceito de engenharia social.
d) Nosso gabarito: ransomware.
e) Conceito de scan.
Letra d.

---

021. (Q2862805/QUADRIX/CRO-MS/ANALISTA ADMINISTRATIVO/2023) Em relação aos conceitos de organização e de gerenciamento de arquivos e de programas, aos procedimentos de segurança da informação e às noções de vírus, worms e pragas virtuais, julgue os itens.
O ransomware, programa similar ao worm, apresenta mecanismos de comunicação com o invasor, os quais permitem que aquele seja remotamente controlado. A principal característica desse programa é a capacidade de se propagar automaticamente pelas redes, com o envio de cópias de si mesmo de um equipamento para outro.

Ransomware é um ataque que consiste em criptografar dados do usuário e solicitar um resgate para fornecer a chave que torna os dados acessíveis novamente.
O programa semelhante ao worm que a questão trouxe é o Bot.
Errado.

---

022. (Q2805091/SELECON/PREF. NOVA MUTUM/INSTRUTOR DE INFORMÁTICA/2023) Um ambiente de rede de computadores sofreu um ataque de um hacker, que consistiu no recebimento de mensagens com endereços IP de origem falsos, de modo que o sistema para o qual o pacote foi direcionado não conseguisse identificar corretamente o remetente. Esse tipo de ataque também é conhecido como:
a) SYN Flood
b) Brute Force
c) IP Spoofing
d) Session Hijack

a) **SYN Flood** é um tipo de ataque DoS com o objetivo de enviar muitas solicitações falsas de conexão para que o servidor fique sobrecarregado processando as solicitações, o que causa a negação do serviço.

b) **Brute Force** (**Força bruta**) é um ataque cibernético que consiste em adivinhar o login (nome de usuário) e a senha do usuário por tentativa e erro. O objetivo do atacante é possuir os mesmos privilégios de acesso do usuário/vítima.
c) Independentemente do tipo de Spoofing, todos possuem a mesma finalidade: **FALSIFICAR a ORIGEM** da mensagem ou dos dados.
d) **Session Hijack** é uma ameaça de segurança cibernética que permite que um atacante assuma o controle de uma sessão de usuário válida em um sistema de computador. Isso pode ser feito roubando o nome de usuário, senha ou outro identificador de sessão do usuário. Uma vez que o atacante assumiu o controle da sessão, ele pode acessar as informações do usuário, modificar suas configurações ou até mesmo executar ações em seu nome.
Letra c.

---

023. (Q2878245/QUADRIX/CAU-TO/AGENTE DE FISCALIZAÇÃO/2023) No que diz respeito aos conceitos de organização e de gerenciamento de arquivos e de pastas, aos sítios de busca e de pesquisa na Internet e às noções de vírus, worms e pragas virtuais, julgue os itens.
Com a finalidade de monitorar computadores e dispositivos, um adware pode atuar como um spyware.

Adware é um software projetado para parecer uma propaganda que, quando utilizado de maneira maliciosa, pode monitorar (ESPIONAR) o tipo de navegação do usuário e direcionar propagandas de acordo com seu histórico de navegação.
Certo.

---

024. (Q2676498/IF-MT/TÉCNICO DE LABORATÓRIO/ÁREA: INFORMÁTICA/2023) Leia as sentenças abaixo.
I. programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento.
II. conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um equipamento comprometido.
III. programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
IV. programa que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado.
As sentenças dizem respeito a códigos maliciosos e são, respectivamente, as definições de:
a) Vírus, Worm, Bot e Rootkit
b) Botnet, Ramsonware, Trojan e Worm

c) Rootkit, Vírus, Trojan e Botnet
d) Worm, Rootkit, Backdoor e Bot
e) Trojan, Worm, Vírus e Rootkit

I – Conceito de worm.
II – Conceito de rootkit.
III – Conceito de backdoor.
IV – Conceito de bot.
Letra d.

---

025. (Q2674596/IADES/SEAGRI-DF/TÉCNICO DE DESENVOLVIMENTO AGROPECUÁRIA/ÁREA AGENTE ADMINISTRATIVO/2023) Uma modalidade comum de ataques cibernéticos se utiliza de programas para edição de texto, planilhas ou apresentações para incluir código malicioso e autorreplicável em rotinas pré-definidas que são incorporadas aos documentos manipulados por esses aplicativos. Essa modalidade de ataque denomina-se
a) vírus de macro
b) SQL injection
c) exploit
d) cavalo de Troia
e) middleware

a) **Vírus de Macro** insere seu código malicioso nos arquivos que possuem macros. Quando o arquivo infectado é executado (aberto), o vírus será executado junto com a macro, o que implicará na infecção do computador.
Esse tipo de vírus infecta os arquivos do Office que contêm macros. Portanto, ao falar em vírus de macro, devem ser mencionados arquivos do Office.
b) **SQL Injection** é uma vulnerabilidade de segurança que permite que um atacante execute comandos SQL arbitrários em um banco de dados. Isso pode ser feito inserindo código SQL malicioso em um formulário web ou em uma consulta SQL. Uma vez que o código SQL malicioso é executado, o atacante pode obter acesso a dados confidenciais, modificar dados ou até mesmo derrubar o servidor.
c) **Exploit** é um ataque que aproveita as vulnerabilidades de um aplicativo, sistema operacional ou até mesmo hardware para assumir o controle do computador ou roubar dados de rede. Ele foi criado para explorar as brechas, permitindo o acesso indevido e não autorizado do invasor, além de possibilitar o acesso remoto ao sistema, acesso a informações confidenciais, interrupção de serviços, entre outros.

d) **Cavalo de Troia** é um tipo de malware que se disfarça como um presente ou aplicativo útil; parece inofensivo, mas traz consigo várias ameaças, como vírus, worms, bots, backdoors e spywares.
e) **Middleware** é um software que facilita a comunicação entre diferentes componentes de um sistema de software. Ele é usado para conectar diferentes sistemas, plataformas e tecnologias. O middleware pode ser utilizado para fornecer uma variedade de serviços.
Letra a.

---

026. (Q2735119/FUNDEP/PREF. LAVRAS/AGENTE DE TRÂNSITO/2023) O tipo de spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento é chamado de
a) Keylogger.
b) Worm.
c) Backdoor.
d) Cavalo de Troia.

a) **Keylogger**: é um spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador.
b) **Worm**: é um malware especializado em explorar vulnerabilidades e tem como objetivo causar negação de serviço.
c) **Backdoor**: é um programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.
d) **Cavalo de Troia**: é um tipo de malware que se disfarça como um presente ou aplicativo útil, parece inofensivo, mas traz consigo várias ameaças, como vírus, worms, bots, backdoors e spywares.
Letra a.

---

027. (Q2703129/FUNDAÇÃO CEFETMINAS/IFB/PROFESSOR/ÁREA: EDIÇÃO/VIDEOGRAFISMO/2023) Qual a descrição do ataque denominado “força bruta”?
a) O atacante sobrecarrega o sistema com inúmeras requisições, forçando o servidor tornar o sistema indisponível.
b) O atacante tenta acesso ao sistema através de tentativa e erro, utilizando como base uma lista de nomes de usuários e senhas aleatórias.
c) Um grupo de atacantes utiliza diversos computadores infectados na internet para que, através de um ataque em massa, ocasione uma indisponibilidade no sistema e a partir de então seja possível assumir o controle.

d) O atacante envia um arquivo para o computador da vítima e, ao ser aberto, o arquivo criptografa todo o sistema da vítima. Por fim, o atacante solicita dinheiro em troca da chave para descriptografar os arquivos.
e) O atacante envia um link malicioso pelo e-mail da vítima. Ao abrir o link, o computador da vítima é bloqueado de maneira forçada.

a) Ataque de DoS
b) Ataque de Força Bruta
c) DDoS
d) Ransomware
e) Ransomware
Letra b.

---

028. (Q2700119/IBADE/FUNDAÇÃO FACELI/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2023) _____ é um ataque que tenta roubar seu dinheiro ou a sua identidade fazendo com que você revele informações pessoais, tais como: números de cartão de crédito, informações bancárias ou senhas em sites que fingem ser legítimos. Assinale a alternativa que preencha a lacuna acima.
a) Pharming
b) Phishing
c) Rootkits
d) Keyloggers
e) Adware

a) O golpe de **Pharming** redireciona o usuário por meio do envenenamento do DNS, o qual passa a traduzir endereços URL para IP fraudulento. O usuário digita o endereço correto na barra de endereços do navegador, mas é redirecionado para um site diferente. O site para o qual o usuário é redirecionado geralmente é um site falso, criado pelo atacante para enganar o usuário a digitar suas informações pessoais. O atacante, então, pode usar essas informações para roubar a identidade do usuário, fazer compras em seu nome ou cometer outros crimes.
b) Conceito de Phishing.
c) **Rootkit** refere-se a um conjunto de programas e técnicas realizadas para esconder e assegurar a permanência do atacante ou até mesmo de outro código malicioso no computador infectado da vítima. Então, se disfarçam como um utilitário ou software de manutenção ou gerenciamento, com o objetivo de obter privilégios de administrador (root).

d) **Keylogger** é um spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador.
e) **Adware** projetado especificamente para exibir anúncios. Ele pode ser usado para fins legítimos, como uma forma de patrocínio ou retorno financeiro, ou para fins maliciosos, como uma forma de rastrear os hábitos de navegação do usuário ou roubar informações pessoais. Adware legítimo geralmente é incluído em programas e serviços com o consentimento do usuário. O adware pode ser usado para gerar receita para os desenvolvedores do programa ou serviço, ou pode ser usado para promover produtos ou serviços relacionados. Por exemplo, um navegador da web pode incluir adware que exibe anúncios para produtos que são relevantes para os interesses do usuário. Adware malicioso, por outro lado, é instalado no computador do usuário sem o seu consentimento. O adware malicioso pode ser usado para rastrear os hábitos de navegação do usuário, roubar informações pessoais ou até mesmo instalar outros malwares. Por exemplo, um programa de adware malicioso pode exibir anúncios que redirecionam o usuário para sites maliciosos ou pode roubar as informações de cartão de crédito do usuário.
Letra b.

---

029. (Q2849791/FUNDEP/CRO-MG/CONTADOR/2023) O código malicioso que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o consentimento do usuário é chamado de
a) Spyware.
b) Cavalo de Troia.
c) Rootkit.
d) Spam.

a) **Spyware** é uma categoria de malware que atua como um espião, coletando dados do usuário sem seu conhecimento ou consentimento. Esses tipos de malware são classificados como spywares devido ao seu propósito de capturar informações pessoais sem o conhecimento do usuário.
b) **Cavalo de Troia** é um tipo de malware que se disfarça como um presente ou aplicativo útil; parece inofensivo, mas traz consigo várias ameaças, como vírus, worms, bots, backdoors e spywares.
c) **Rootkit** refere-se a um conjunto de programas e técnicas realizadas para esconder e assegurar a permanência do atacante ou até mesmo de outro código malicioso no computador infectado da vítima. Esses programas se disfarçam como utilitários ou softwares de manutenção ou gerenciamento, com o objetivo de obter privilégios de administrador (root).

d) **Spam** é a mensagem eletrônica NÃO SOLICITADA, geralmente enviada para um grande número de pessoas.
Letra b.

---

030. (Q2729926/INQC/COMDEP/ASSISTENTE ADMINISTRATIVO/2023) No caso de um usuário de computador estar diante de um ataque, no qual o atacante cria uma aparência de que as comunicações oriundas dele vêm de uma fonte confiável, diz-se que o usuário sofreu um ataque denominado:
a) dialer
b) synflood
c) spoofing
d) keylogger

a) **Dialer** é um programa de computador projetado para discar números de telefone. Ele é usado para fazer chamadas telefônicas, enviar mensagens de texto e outras funções relacionadas ao telefone.
b) O **SYN Flood** é um tipo de ataque DoS com o objetivo de enviar muitas solicitações falsas de conexão para que o servidor fique sobrecarregado processando as solicitações, o que causa a negação do serviço.
c) **Spoofing** é um crime cibernético em que o atacante tenta se passar por uma pessoa conhecida dos contatos ou por instituições reconhecidas, com a finalidade de ganhar a confiança do usuário. O objetivo desse ataque consiste em obter acesso às informações e contornar medidas de segurança.
d) **Keylogger** é um spyware capaz de capturar as teclas digitadas pelo usuário no teclado físico do computador.
Letra c.

---

031. (Q4284426/QUADRIX/SES-SP/TÉCNICO DE ENFERMAGEM/2026) Um malware infectou um computador da rede hospitalar e, diferentemente de um vírus comum que precisa ser executado pelo usuário (clicando em um arquivo), este programa malicioso começou a se replicar automaticamente através das falhas de segurança da rede, infectando dezenas de outras máquinas conectadas em questão de minutos, sem nenhuma intervenção humana. Com base nessa situação hipotética, assinale a opção que apresenta a classificação específica dessa praga virtual que se propaga autonomamente pela rede.
a) trojan
b) ransomware

c) adware
d) worm
e) keylogger

A característica da autorreplicação ou replicação automática define de forma inconfundível o worm, especialmente ao explorar falhas de segurança da rede, por onde ele se propaga. Outra característica que define o worm é o fato de não necessitar de intervenção humana. O worm também tem a capacidade de infectar diversas outras máquinas em poucos minutos. Embora a questão não mencione, o worm também visa inutilizar as máquinas, tirando-as de serviço ou funcionamento.

Letra d.

---

032. (Q4296858/INSTITUTO AOCP/SEJUSP-MG/POLICIAL PENAL/2026) Durante o turno vespertino na sala de controle de acesso de uma unidade prisional, o policial penal recebe diversas notificações sobre acessos irregulares ao sistema interno e tentativas de login feitas com credenciais de servidores que não estavam de plantão. Após verificação, constata-se que todos os usuários afetados haviam utilizado o mesmo computador recentemente. Não há evidências de e-mails fraudulentos nem de arquivos criptografados, e o terminal aparentemente funciona de forma normal. Considerando as principais ameaças digitais e seus modos de atuação, é correto afirmar que o incidente descrito retrata a ameaça de um

a) keylogger, programa espião que registra silenciosamente todas as teclas digitadas, capturando logins e senhas inseridos no terminal para posterior envio ao invasor.
b) phishing, golpe eletrônico que simula comunicações legítimas e induz o usuário a informar suas credenciais em um site falsificado.
c) ransomware, software malicioso que criptografa os dados do sistema e exige pagamento para liberar o acesso aos arquivos.
d) sniffer, ferramenta usada para interceptar pacotes de dados na rede local, capturando informações transmitidas sem criptografia.

O enunciado da questão afirma que as credenciais de diversos usuários foram capturadas e estavam sendo utilizadas por outros usuários, pois coincidiam com horários em que seus titulares não estavam presentes na instituição. Dentre as alternativas, a única ameaça que retrata esse tipo de ação é o keylogger, pois ele é capaz de capturar as credenciais ao serem digitadas suas senhas por meio do teclado físico.

Letra a.

---

033. (Q4299042/FGV/AMAZUL/ESPECIALISTA DE RADIOPROTEÇÃO/2026) No contexto de segurança da informação, mais especificamente sobre malwares, associe corretamente o cada item numerado no primeiro bloco (variando de 1 a 4) às lacunas do segundo bloco.

1. Cavalo de Troia (trojan horse) **2**. Verme (worm) **3**. Bomba lógica (logic bomb) **4**. Zumbi (zumbi, bot)	( ) Execução autônoma com capacidade de replicação automática e propagação entre sistemas conectados. ( ) Malware ativado por condição predefinida após período hibernado. ( ) Ataque a outras máquinas executado por software malicioso instalado em host comprometido. ( ) Software aparentemente útil que possui desvio oculto e malicioso de finalidade.

Assinale a opção que corretamente associa o nome do malware no primeiro bloco e a característica apresentada no segundo bloco.

a) 1 – 2 – 4 – 3
b) 4 – 1 – 3 – 2
c) 2 – 3 – 4 – 1
d) 1 – 3 – 2 – 4
e) 3 – 4 – 2 – 1

1. **Cavalo de Troia** (**trojan hors**e) – Software aparentemente útil que possui desvio oculto e malicioso de finalidade.
2. **Verme** (**worm**) – Execução autônoma com capacidade de replicação automática e propagação entre sistemas conectados.
3. **Bomba lógica** (**logic bom**b) – Malware ativado por condição predefinida após período hibernado.
4. **Zumbi** (**zombie**, **bot**) – Ataque a outras máquinas executado por software malicioso instalado em host comprometido.

Letra c.

---

034. (Q4272276/QUADRIX/CRQ 7/ASSISTENTE ADMINISTRATIVO/2026) Em relação aos conceitos de redes de computadores, às noções de vírus, worms e pragas virtuais e aos conceitos de inteligência artificial (IA), julgue os itens seguintes.

O ransomware é uma praga virtual que tem como principal característica capturar dados pessoais do usuário e utilizá-los para enviar spam sem solicitar permissão.

O ransomware é uma praga virtual que tem como principal característica criptografar os dados ou a máquina do usuário, impedindo-o de acessá-los e cobrando pelo resgate (ransom) da chave criptográfica que decodifica os dados.

Errado.

---

035. (Q4386081/QUADRIX/CRF-DF/ADMINISTRADOR/2026) Acerca de redes de computadores, antivírus e computação em nuvem, julgue os itens a seguir.

Todo malware que executa código automaticamente sem intervenção do usuário é classificado como vírus.

É totalmente errado classificar outros malwares como vírus, pois os vírus possuem características muito específicas, como, por exemplo, inserir cópias de si mesmos em outros arquivos e se replicar por meio dessa infecção. Além disso, uma característica que define os vírus é o fato de não serem automáticos ou autônomos, pois dependem da intervenção humana para serem ativados.

Errado.

---

036. (Q4383739/CEBRASPE-CESPE/Câmara dos Deputados/Analista Legislativo/Área: Processo Legislativo e Gestão/2026)Julgue os itens seguintes, relativos a procedimentos de backup, vírus e worms, soluções anti-spyware e ameaças pharming.

O pharming caracteriza-se pela manipulação direta do conteúdo apresentado ao usuário no navegador por meio de código malicioso, com atuação associada à modificação dinâmica de páginas durante a sessão.

O malware descrito na questão é o hijacker, também chamado de sequestrador de navegador. Sua principal característica é injetar código malicioso no navegador, alterando dinamicamente o conteúdo das páginas durante a navegação. Ele manipula resultados, anúncios, formulários ou redirecionamentos enquanto a sessão está ativa.

Errado.

---

037. (Q4328132/FGV/ALE-GO/POLICIAL LEGISLATIVO/2026) Durante uma busca na internet por informações sobre um edital de licitação, um Assessor Legislativo da ALE-GO acessou um site de notícias. Na lateral da página, um anúncio chamativo dizia:

SEU COMPUTADOR PODE ESTAR INFECTADO! CLIQUE AQUI PARA VERIFICAR AGORA!

O Assessor Legislativo percebeu que o site principal era confiável, mas desconfiou desse anúncio específico. A sua desconfiança é fundamentada no fato de que esse tipo de anúncio é comumente associado a uma prática maliciosa específica que é conhecida como

a) Phishing
b) Spam
c) Ransomware
d) Backdoor
e) Scareware

Scareware é um tipo de software malicioso projetado para assustar (“scare”) o usuário e levá-lo a tomar decisões impulsivas – geralmente, pagar por um programa falso ou clicar no link indicado para instalar algo perigoso.

Letra e.

---

038. (Q4284410/QUADRIX/SES-SP/FISIOTERAPEUTA/2026) Todos os funcionários do hospital receberam um e-mail com o logotipo do banco que processa a folha de pagamento, informando: “Seus dados cadastrais estão desatualizados e seu salário será bloqueado. Clique AQUI para atualizar imediatamente”. O link direcionava para um site falso, visualmente idêntico ao do banco, projetado para roubar a senha do usuário.Com base nessa situação hipotética, assinale a opção que apresenta o nome técnico desse tipo de fraude com base em engenharia social.

a) DDoS
b) phishing
c) hoax
d) furto de identidade
e) brute force

Essa ameaça se parece muito com a da questão anterior; porém, a principal diferença é que a atual é enviada por e-mail e o link da mensagem direciona o usuário para uma página falsa, na qual o usuário fornecerá seus dados ao golpista.

Letra b.

---

039. (Q4299458/FGV/AMAZUL/TÉCNICO DE INFORMÁTICA/2026) O uso de programas maliciosos (malwares) em crimes cibernéticos é cada vez mais associado a objetivos bem específicos, como espionagem, fraude financeira, controle remoto de máquinas e fraudes

correlatas. Considerando os diferentes tipos de malware e seus objetivos principais, assinale a opção que corretamente indica o nome do malware que tem como propósito sequestrar a máquina e exigir, por extorsão, o pagamento de resgate.
a) Backdoor
b) Banking Trojans
c) Bots
d) Malware APT
e) Ransomware

O Ransomware é um malware que tem como principal característica criptografar os dados ou a máquina do usuário, impedindo-o de acessá-los e cobrando pelo resgate (ransom) da chave criptográfica que decodifica os dados.
a) **Backdoor** – malware que abre vulnerabilidades e se mantém oculto, permitindo acesso remoto não autorizado ao sistema.
b) **Banking Trojans** – malware disfarçado de aplicativo útil, porém projetado para roubar credenciais e dados bancários do usuário.
c) **Bots** – softwares maliciosos, variantes dos worms, que executam ações automatizadas sob controle de um atacante.
d) **Malware APT** – APT significa ***Advanced Persistent Threat*** (Ameaça Avançada Persistente). Esse malware é um código malicioso avançado criado para infiltrar-se discretamente e manter acesso prolongado a um alvo específico.
Letra e.

---

040. (Q4299526/FGV/AMAZUL/TÉCNICO DE INFORMÁTICA/2026) Durante um incidente, a equipe detecta um programa que se replica automaticamente explorando falhas em serviços de rede internos. O tipo de malware descrito por esse comportamento é
a) Worm
b) Vírus
c) Cavalo de Troia
d) Spyware
e) Backdoor

a) **Worm** – malware que se replica automaticamente pela rede, sem depender de arquivos hospedeiros.
b) **Vírus** – código malicioso que se anexa a arquivos legítimos e se espalha quando eles são executados.

c) **Cavalo de Troia** – programa que aparenta ser legítimo, mas esconde uma função maliciosa.
d) **Spyware** – software oculto que coleta informações do usuário sem consentimento.
e) **Backdoor** – mecanismo oculto que permite acesso remoto não autorizado ao sistema.
Letra a.

---

041. (Q3779541/QUADRIX/CRF-MS/ASSISTENTE ADMINISTRATIVO/2025) Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.
Um vírus de computador é um(a)
a) programa malicioso que se replica, anexando-se a arquivos executáveis e depende da ação do usuário para se espalhar.
b) componente do sistema operacional que impede a instalação de softwares não autorizados.
c) programa autônomo que se espalha automaticamente pela rede, sem intervenção do usuário.
d) ferramenta de segurança que monitora e corrige falhas do sistema.
e) um arquivo de dados sensíveis e ilegais.

Um vírus é um programa malicioso que se replica, inserindo cópias de si mesmo em outros arquivos executáveis, anexando-se a eles e dependendo da ação do usuário para ser ativado e se espalhar.
Letra a.

---

042. (Q4138304/QUADRIX/CORE-SE/CONTADOR/2025) Um usuário percebeu que a tela do seu computador estava abrindo diversos anúncios em janelas "pop-ups", mesmo quando não estava navegando em sites suspeitos. Além disso, o navegador teve sua página inicial e seu mecanismo de busca alterados sem sua permissão. Com base nessa situação hipotética e considerando os vírus, worms e outras pragas virtuais, assinale a opção que apresenta o tipo de malware que causa esse comportamento.
a) ransomware
b) adware
c) keylogger
d) worm
e) rootkit

O adware é um tipo de software malicioso que exibe **anúncios indesejados** no dispositivo do usuário, podendo também coletar dados de navegação sem autorização e ser classificado como um tipo de spyware.

Letra b.

---

043. (Q4061424/QUADRIX/CRO-SP/AUXILIAR ADMINISTRATIVO/2025) Quanto ao uso de webmails, ao armazenamento em nuvem e às noções de vírus, worms e pragas virtuais, julgue os itens seguintes.

Um spyware, diferentemente de um vírus, tem como objetivo principal a replicação automática e o comprometimento de arquivos do sistema operacional.

Um spyware é um software malicioso oculto que coleta informações do usuário sem consentimento e as envia ao atacante.

Errado.

---

044. (Q4132847/CEBRASPE-CESPE/TCE-RS/OFICIAL DE CONTROLE EXTERNO/ÁREA: OFICIAL INSTRUTIVO/2025) No que se refere a armazenamento de dados na nuvem, pragas virtuais e firewall, julgue os itens subsequentes.

Spyware é um programa que se replica ao infectar arquivos ou documentos que contenham código executável.

Essa questão é muito parecida com a anterior, não é mesmo? Mas, como vimos, o spyware é um malware que infecta o dispositivo sem o conhecimento do usuário e captura seus dados sem o consentimento deste, transmitindo-os ao atacante.

Errado.

---

045. (Q4288713/INSTITUTO AOCP/UENF/TÉCNICO EM NÍVEL SUPERIOR/ÁREA: BIBLIOTECA/2025) A segurança na internet envolve uma série de práticas e tecnologias que visam proteger usuários, dispositivos e dados durante o uso de redes digitais, com o objetivo de prevenir fraudes, invasões e roubos de informações. Dentro desse contexto, há diversas ameaças e técnicas usadas para comprometer a segurança. Sabendo disso, assinale a alternativa que descreve uma técnica de manipulação psicológica voltada para enganar usuários e obter dados confidenciais, como senhas ou informações bancárias.

a) Spoofing
b) Criptografia
c) Rootkit
d) Certificado digital
e) Engenharia social

A Engenharia Social é uma técnica humana de persuasão que visa ludibriar o usuário e convencê-lo a realizar ações de seu interesse, como fornecer seus dados pessoais sigilosos, geralmente bancários.

Letra e.

---

046. (Q4377334/INSTITUTO AOCP/IF-PB/TÉCNICO EM ASSUNTOS EDUCACIONAIS/2025) O malware conhecido como Cavalo de Troia (Trojan) é amplamente utilizado por atacantes. Sua característica definidora não é o método de replicação, mas sim a sua forma de distribuição e execução inicial. O Cavalo de Troia se distingue dos Vírus e Worms

a) pela sua capacidade de se replicar automaticamente pela rede, explorando vulnerabilidades sem a interação do usuário.
b) porque sua principal ação é criptografar arquivos do sistema operacional para exigir um pagamento de resgate.
c) porque, no Trojan, o código malicioso se anexa a arquivos executáveis legítimos e se espalha junto com eles.
d) porque ele se disfarça de programa legítimo e, dessa forma, é útil para enganar o usuário a instalá-lo voluntariamente, criando uma porta de acesso.
e) porque ele opera no nível de kernel do sistema operacional para ocultar a presença de outros softwares maliciosos.

a) **Worm** – possui a capacidade de se replicar automaticamente pela rede, explorando vulnerabilidades sem a interação do usuário.
b) **Ransomware** – sua principal ação é criptografar arquivos do sistema operacional para exigir um pagamento de resgate.
c) **Vírus** – código malicioso que se anexa a arquivos executáveis legítimos e se espalha junto com eles.
d) **Trojan** – disfarça-se de programa legítimo e, dessa forma, é útil para enganar o usuário a instalá-lo voluntariamente, criando uma porta de acesso.
e) **Rootkit** – opera no nível de kernel do sistema operacional para ocultar a presença de outros softwares maliciosos.

Letra d.

---

047. (Q3979898/CEBRASPE-CESPE/CAESB/OPERADOR DE ESTAÇÃO DE TRATAMENTO/2025) Certo dia, Paulo recebeu um email que pensou ter sido enviado pelo banco. Ele foi informado que sua conta tinha sido comprometida e que seria necessário clicar no link fornecido para bloquear o acesso das informações pessoais a terceiros de má-fé. Ao clicar, Paulo foi direcionado a um site falso, idêntico ao do banco, e inseriu os dados que criminosos cibernéticos precisavam para que tivessem acesso à conta. Considerando as informações na situação hipotética precedente, assinale a opção que corresponde ao tipo de golpe digital aplicado em Paulo.

a) phishing
b) spyware
c) ransomware
d) vírus
e) trojan

O phishing geralmente utiliza o e-mail simulando uma instituição conhecida como veículo de propagação. Em sua mensagem, ele dispõe de um link que direciona o usuário para uma página falsa, na qual o usuário fornece seus dados, que serão enviados ao atacante.

Letra a.

---

048. (Q3765330/CEBRASPE-CESPE/AEB/TECNOLOGISTA JÚNIOR/ÁREA: TECNOLOGIA DA INFORMAÇÃO/2025) Um malware projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros é do tipo

a) trojan
b) ransoware
c) adware
d) rootkit
e) spyware

Um spyware é um software malicioso que atua de forma oculta, coletando informações do usuário sem autorização e transmitindo esses dados ao atacante.

Letra e.

---

049. (Q3938162/IADES/CRMV-PI/TÉCNICO ADMINISTRATIVO/2025) Uma prática maliciosa comum na internet consiste no envio de e-mails fraudulentos que tentam se passar por comunicações de empresas ou instituições conhecidas para enganar o usuário e induzi-lo a fornecer dados pessoais e senhas. Esse tipo de golpe é conhecido como

a) adware.
b) spam.
c) firewall.
d) phishing.
e) spyware.

O phishing costuma utilizar e-mails que imitam instituições legítimas como meio de disseminação, incluindo um link que direciona a vítima a uma página falsa onde, ao inserir seus dados, estes são capturados e enviados ao atacante.
Letra d.

---

050. (Q3915018/CEBRASPE-CESPE/FUB/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2025)
Em relação a vírus e antivírus, julgue os itens seguintes.
Rootkit é um tipo de vírus que liberam acesso ao computador para softwares não autorizados.

Um rootkit não é um vírus, mas sim um conjunto de ferramentas maliciosas (malware) criado para esconder processos, arquivos, chaves de registro, conexões de rede e até outros malwares, garantindo que a infecção permaneça invisível para o usuário e para soluções de segurança tradicionais.
Errado.

Conclusão:

Chegamos, assim, ao fim dessa maratona de questões! Espero que você tenha gabaritado todas elas. Ah! Faz o seguinte agora: vai lá nas avaliações dessa aula, diz para mim o quanto você gostou dela e quantas questões você gabaritou, beleza? Eu lerei sua avaliação assim que você a fizer, pois leio todos os comentários das avaliações dos meus alunos!

Se você quiser fazer parte da minha rede social, aponte sua câmera para o QR Code à esquerda e siga-me:

@PROF.MAURICIOFRANCESCHINI

INFORMÁTICA PARA CONCURSOS
CURSO COMPLETO
Professor: Maurício Franceschini
(CÓDIGO: 149083)

E se quiser acessar meu curso completo de informática para concursos, aponte sua câmera para o QR Code à direita.

Parabéns por ter chegado até aqui! Parabéns por não ter desistido e por ter terminado todas as questões! Você é uma pessoa vencedora, uma verdadeira campeã!

Estou muito orgulhoso de você!

REFERÊNCIAS

Cartilha de Segurança para Internet – Versão 4.0 (cert.br)

Educa Mais Brasil

Entenda o que é catfishing, golpe que levou atleta italiano a acreditar que namorava Alessandra Ambrosio por 15 anos (globo.com)

O que é bomba lógica? Examplos e prevenção | Avast

O que é malvertising e como impedir malware de anúncios? | Avast

O que é spoofing? | E-mail, IP etc.| Definição de spoofing | AVG

O que é um exploit de computador? | Definição de exploit | Avast

O que é um sniffer? | Como se proteger contra sniffers | Avast

O que são cookies? | Os cookies prejudicam a privacidade? (kaspersky.com.br)

Os hackers mais destemidos da história (canalcienciascriminais.com.br)

Os hackers mais perigosos do mundo – Segredos do Mundo (r7.com)

Abra

caminhos

crie

futuros

gran.com.br