

**Disciplina: Segurança de Sistemas**

**Profa.: Rejane Cunha Freitas (**rejane.freitas@faculdadecdl.edu.br**)**

**Pesquisa e diferencie os seguintes tipos de malware** (sua resposta para cada termo deve ter no mínimo cinco e no máximo dez linhas). Não se esqueça de indicar ao final as referências de suas fontes de pesquisa.

Spyware: Spywares são programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. Todavia, isto não significa que eles sejam em sua totalidade programas maus. Existem sim, muitos spywares de má índole, criados para coletar informações pessoais e, com elas, praticar atividades ilegais. Entretanto, nem todos são assim. Muitas vezes, envolve a coleta de dados confidenciais, como senhas, PINs e números de cartões de crédito, o monitoramento de pressionamentos de teclas, o rastreamento de hábitos de navegação e a coleta de endereços de e-mail.

Adware: Adware é um software indesejado projetado para jogar anúncios em sua tela, na maioria das vezes dentro de um navegador da Web. Alguns profissionais de segurança o enxergam como o precursor moderno do PUP (programa potencialmente indesejado). Normalmente, ele usa um método furtivo para disfarçar-se como legítimo ou se sobrepõe em outro programa para ludibriá-lo a instalá-lo em seu PC, tablet ou dispositivo móvel.

Bot: Um 'bot' é um programa de software que executa tarefas automatizadas, repetitivas e pré-definidas. Os bots normalmente imitam ou substituem o comportamento do usuário humano. Por serem automatizados, operam muito mais rápido do que os usuários humanos. Eles realizam funções úteis, tais como serviço ao cliente ou indexação de motores de busca, mas também podem vir sob a forma de malware – usado para obter controle total sobre um computador.

Ransomware: Ransomware é um software nocivo que é usado para bloquear dados de computadores e servidores através do uso de algum tipo de criptografia. Esse malware é usado por hackers para exigir resgates, normalmente cobrado em criptomoedas como o bitcoin, para que os dados sejam novamente liberados. Apesar do Ransomware também ser um malware, ele não possui a capacidade de auto-replicação de um vírus. Enquanto a propagação de um vírus acontece de forma espontânea e sem controle, o Ransomware é um código malicioso distribuído via internet que criptografa os arquivos de computadores através da exploração de vulnerabilidades encontradas nos sistemas operacionais.

Scareware: Scareware é um tipo de software malicioso que indica que existe algo errado com o computador e tenta convencer o usuário a fazer o download de um programa de proteção. Geralmente, esses avisos costumam aparecer em forma de pop-up em sites como falsos programas antivírus que se parecem muito com as caixas de diálogo geradas pelo Centro de Segurança do Sistema Operacional.

Rootkit: Basicamente é um programa de computador ilegal projetado para fornecer acesso privilegiado contínuo a um computador e esconder sua presença. O termo rootkit é uma conexão das duas palavras “root” e “kit”. Originalmente, um rootkit era uma coleção de ferramentas que habilitava o acesso no nível de administrador a um computador ou rede. A termo “root” refere-se à conta de administração em sistemas Unix e Linux, e “kit” refere-se aos componentes de software que implementam a ferramenta. Atualmente, os rootkits geralmente estão associados a malwares – como trojans, worms, vírus – que escondem sua existência e ações dos usuários e outros processos do sistema.

Worms: Um Worm é um programa semelhante aos vírus, com a diferença de este ser auto-replicante, ou seja, ele cria cópias funcionais de si mesmo e infecta outros computadores. Tal infecção pode ocorrer através de conexões de rede locais, Internet ou anexos de emails. Alguns worms infectaram centenas de computadores por meio das redes sociais MySpace e Facebook. Alguns worms são usados para criar brechas nos computadores e torná-los alvo fácil para a entrada de outros worms. Os computadores infectados funcionam como “zombies” e são usados por pessoas que enviam spam para encaminhar emails contaminados ou atacar endereços de sites da Internet.

Vírus: Vírus de Computador é o inimigo número um de todos que possuem um desktop, notebook, tablet e até mesmo smartphone. Sua construção é simples mas pode ser devastadora. O Vírus é um software desenvolvido com base em características diversas e com inúmeros "temas". É chamado por muitos de software malicioso, tal qual um vírus que infecta o sistema e se espalha para outros computadores de forma muito rápida, através de links, e-mails e arquivos infectados. A sua dispersão se dá muitas vezes pela própria ação do usuário, o qual executa o arquivo sem saber de sua procedência e má intenção.

Cavalo de Tróia: Um Cavalo de Troia oculta um malware em um arquivo aparentemente normal. A maioria dos Cavalos de Troia tem como objetivo controlar o computador de um usuário, roubando dados e inserindo outro malware no computador de suas vítimas. Os Cavalos de Troia não são um problema somente para computadores desktops e notebooks. Eles podem também afetar dispositivos móveis. Em geral, um Cavalo de Troia vem anexado a um programa que aparenta ser legítimo, porém é uma versão falsa do aplicativo, carregada com malware. Esses criminosos cibernéticos normalmente o colocam em mercados de aplicativos piratas ou informais, para que usuários inocentes façam o seu download.

Bombas lógicas: Uma bomba lógica é um código malicioso que os hackers inserem em uma rede de computadores, programa de software ou dispositivo digital. Este código permanece adormecido até ser acionado por uma determinada condição. Quando a bomba é disparada, ela “explode” e causa estragos no sistema do seu computador. O que o torna mais perigoso é que ele pode detonar repetidamente antes que você perceba.

**Pesquise também o que são :**

Spam: SPAM é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. O SPAM tem um fundo geralmente comercial, mas também pode assumir um viés criminoso. Na maioria dos casos, a mensagem de SPAM promove algum produto ou serviço.

Phishing: O phishing é um tipo de ciberataque que se assemelha a uma tentativa de enganar usuários da tecnologia digital. Geralmente ocorre via e-mail, mas também pode aparecer em forma de ligações, mensagens em redes sociais e SMS. Frequentemente os autores se disfarçam de alguém que você conhece ou de uma instituição conhecida, como um banco, uma marca famosa ou qualquer instituição legítima para atrair indivíduos. O objetivo é conseguir o fornecimento de dados confidenciais, como informações de identificação pessoal, dados bancários e senhas.

Plugins: Plugins são adições ou alterações de software que permitem a personalização de programas de computador, aplicativos e navegadores da web, bem como a personalização do conteúdo oferecido pelos sites. Embora os plugins continuem a ser usados como complementos para personalizar programas e aplicativos, seu uso em navegadores da web diminuiu um pouco, em favor do uso das extensões de navegador.

**Referências:**

<https://www.tecmundo.com.br/spyware/29-o-que-e-spyware-.htm>

<https://www.kaspersky.com.br/resource-center/threats/spyware>

<https://br.malwarebytes.com/adware/>

<https://www.kaspersky.com.br/resource-center/definitions/what-are-bots>

<https://www.controle.net/faq/o-que-e-ransomware>

<https://www.certifiquei.com.br/scareware/>

<https://tripla.com.br/o-que-e-um-rootkit/>

<https://www.tecmundo.com.br/antivirus/206-o-que-e-um-worm-.htm>

<https://www.infoescola.com/informatica/virus-de-computador/>

<https://br.norton.com/internetsecurity-malware-what-is-a-trojan.html>

<https://tecnoguia.istocks.club/o-que-e-malware-logic-bomb-e-como-voce-pode-evita-lo/2021-04-18/>

<https://www.techtudo.com.br/noticias/2016/07/o-que-e-spam.ghtml>

<https://www.psafe.com/blog/o-que-e-phishing/>

<https://tecnoblog.net/responde/o-que-e-um-plugin/>