MALWARES	MALWARES
O que são **Malwares**?	**Malwares:** Ou **"Malicious Ware"**, são rotinas maliciosas criadas com o objetivo de invadir um sistema de informação. São desenvolvidos por Crackers que têm o objetivo de encontrar "brechas" (Cracks) sejam nos sistemas informatizados seja por através dos usuários do sistema com o objetivo de roubar dados, ter acesso a informações confidenciais ou danificar ativos físicos ou lógicos.
Quais os **tipos mais conhecidos** de Malwares?	**- Vírus** **- WORWS** **- Trojan (Cavalo de Tróia);** **- Bots e Botnets;** **- Ransomware;** **- Rootkit;** **- Backdoor;** **- Spyware;** **- Sniffer;** **- Port Scanner;**
O que é um **Vírus de Computador**?	**Vírus de Computador:** É um programa malicioso, ou parte de um programa, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas ou arquivos. Isso faz com que os vírus de computador tenham pelo menos duas características básicas para poder agir: 1) Se replicar sozinhos; 2) Precisam de um hospedeiro, um arquivo que os comporte; Ele NÃO É ativado assim que entra no computador, ele **fica encubado** em algum arquivo dentro do disco rígido, como se fosse um vírus real, e **só é acionado quando o usuário sem saber executa justamente arquivo onde o vírus estava escondido,** levando o vírus para a memória RAM e consequêntemente para o processador.
Quais seriam alguns tipos de Vírus de Computador?	**- Vírus Propagado por e-mail:** envia e-mails para todos os contatos de um endereço de e-mail infectado, Por exemplo: **Vírus Melissa**; - **Vírus de Boot:** é um vírus que se aloja geralmente em aparelhos que podem ser acessados pelo boot do computador e gerem como o sistema operacional deve se comportar. Esses vírus se alocam geralmente em pen drivers, HDs, CDs e DVDs, todos dispositivos que podem ser lidos pelo sistema boot da máquina e dar acesso ao controle do sistema operacional causando grandes estragos; **- Vírus de Script:** são vírus encubados dentro de uma página Web, geralmente eles pedem que o usuário tome alguma ação que resultará na execução do vírus; **- Vírus de Macro:** são vírus criados para atacar diretamente arquivos do Office, que utilizam macros em seus sistema de programação, como: word, excel, access, power point e etc. (alguns podem afetar até arquivos do Libre Office); **- Vírus de Celular:** que se propagam por através de tecnologias comuns em smartphones, como tecnologias bluetooth, SMS, 4G e etc;
- reservado para a questão acima -	
O que é um **WORM**?	**WORM:** Do inglês **"Verme"** é um malware que, assim como os vírus de computador tem a capacidade de se propagar para infectar diversos computadores, porém ele é ainda mais perigoso, pois diferente dos vírus de computador ele PODE SE REPLICAR SOZINHO, porém, ele NÃO PRECISA DE UM HOSPEDEIRO, isso faz com que ele não precise ser executado somente quando o usuário clica em um arquivo que contenha o vírus encubado, ele é executado assim que entra no computador por através das redes. Pois eles são ativados pelos dispositivos responsáveis pelos Protocolos de Internet como o IP, TCP, OSPF e outros, geralmente eles são ativados por roteadores, servidores, nat e outros. Alguns exemplos de WORMS são: **- I Love You:** transmitido pela rede como se fosse uma mensagem de amor, mas replicava-se sobre o HD da vítima acrescentando códigos a chaves de registro do sistema operacional; **- NIMDA:** Ou ADMIN de trás para frente, acessa ao administrador e deixa o sistema todo lento, embora possa atacar qualquer tipo de computador, seu foco é atacar servidores; **- Code Red e Code Red II:** seu foco era explorar uma vulnerabilidade de buffer dos windows 2000 e windows NT, sobrecarregando os buffers desses sistemas;
- reservado para a questão acima -	
O que é um **BOT** e **BOTNET**?	**BOT e BOTNET:** A palavra BOT vêm de **Robot**, esse tipo de malware é colocado sobre o computador de uma vítima com o objetivo de controlar o computador da vítima para que ele faça ações maliciosas sobre um computador alvo - o computador infectado é vulgarizado como **"Computador Zumbi"** por que ele é controlado remotamente como se fosse um Robô - um bom exemplo do uso de BOTs é quando um computador de uma empresa é usado para ter acesso a servidores de uma empresa. Quando um BOT consegue ser instalado em vários computadores em rede temos o BOTNET (Rede de Robôs), onde criminoso terá vários computadores sobre o seu comando para executar a invasão.
O que é um **Trojan**?	**Trojan (Cavalo de Tróia):** Do inglês **(Troianos)**, é um malware que faz referência ao **"Cavalo de Tróia"**, famoso por simular um presente que na verdade era uma armadilha. São malwares dissimulados dentro de arquivos e programas, que ao serem baixados aparentam não ter problema nenhum, inclusive funcionam normalmente, mas por debaixo da programação executam rotinas maliciosas como apagamento de dados, invasões e etc.
O que é um **Ransomware**?	**Ransomware:** Do inglês **"Estilo Sequestrador"**, esse é um malware que "sequestra" os dados de uma pessoa por criptografar os dados e exigir um resgate em troca por enviar uma mensagem na tela dizendo: "Seus dados foram criptografados, pague o resgate em tanto tempo..." e apresenta um timer na tela, caso a vítima não pague o resgaste o criminoso não entregará a chave de descriptografia para a vítima e os dados dela ficarão perdidos. Geralmente os sequestradores exigem pagamento em criptomoedas que são mais difíceis de rastrear do que transferências bancárias. Um método usado para evitar esse tipo de problema é o uso de backup.

MALWARES	MALWARES
O que é um **Rootkit**?	**Rootkit:** É um malware que se esconde no sistema **Root de um sistema operacional**, que seria o administrador do sistema, ele faz isso para esconder seus rastros o máximo possível, pois uma vez escondido no Root ele consegue diblar melhor aplicações de monitoramento anti rotinas maliciosas. Quando o criminoso deseja executar uma invasão, ele utiliza um **"kit de ferramentas"**, armazenados no malware, para assumir o controle diretamente sobre o administrador do sistema, compromento rotinas importantíssimas para o sistema operacional.
O que é um **Backdoor**?	**Backdoor:** Do inglês **"Porta dos Fundos"**, é quando um criminoso invade um computador e instala nele um malware para facilitar uma segunda invasão. Os Backdoors são usados por Crackers que tiveram grande dificuldade ao adentrar um sistema e para não passaram por todo esse trabalho novamente, instalam um Backdoor para facilitar outras invasões.
O que é um **Spyware**?	**Spyware:** Do inglês **"Estilo Espião"**, esse é um malware espião, usado para monitorar as atividades de um computador alvo, ele é usado específicamente para bisbilhotar um computador. Existem alguns tipos específicos de Spyware para capturar coisas diferentes, por exemplo: **- Spyware Keylogger:** captura o que se digita por teclado e envia para o criminoso; **- Spyware Screenlogger:** tira um printScreen da tela quando a vítima clica na tela e envia os printScreens para o criminoso; **- Adware:** envia propagandas para o usuário quando ele acessa um programa; **OBS: existem Spywares legítimos também, quando uma pessoa por vontade própria instala um spyware para monitorar seu computador.**
- reservado para a questão acima -	
O que é um **Hijackers**?	**Hijackers:** Ou "Sequestradores", é um malware que altera o comportamento do browser da máquina, fazendo-o acessar sites por vontade própria, sem que o usuário tenha dado nenhum comando.
O que é um **Sniffer**?	**Sniffer (Farejador):** é um malware instalado no próprio computador do criminoso para **espionar os pacotes de rede Ethernet transitados na rede**, como os quadros Ethernet são endereçados diretamente para computadores específicos, os computadores que não forem os destinatários não escutam as mensagens. O Sniffer faz o contrário, ele faz com que o computador escute todas as mensagens transitadas na Ethernet - chamamos isso de **"modo promíscuo"**. Obviamente esse tipo de ataque seria efetivo somente numa rede distribuída por hub, pois os switches já distribuem os pacotes unicast diretamente ao destinatário.
O que é um **Port Scanner**?	**Port Scanner:** Do inglês **"Varredura de Porta"**, é um malware também instalado no computador do criminoso que tem por objetivo espionar as portas do computador da vítima na busca por brechas que poderiam facilitar um ataque. Ele faz uma varredura buscando as portas mais utilizadas pela vítima, e estuda as vulnerabilidades destas portas, com o objetivo de invadí-las.