**Cavalo de troia**

Cavalo de troia é um tipo de malware que possibilita uma maneira de acesso remoto ao computador após a infecção. Além de executar as funções pelas quais ele foi projetado, também pode fazer outras funções maliciosas, como por exemplo:

* Instalação de keyloggers ou screenlogger;
* Furto de senhas e outras informações;
* Inclusão de backdoors, onde uma pessoa pode ter o total controle sobre o computador;
* Alteração ou exclusão de arquivos;

Para ser instalado no computador o cavalo de troia tem que ser executado, onde geralmente ele vem anexado em um e-mail ou disponível em algum site da internet.

**Worn**

Os worns(ou vermes) é um tipo de malware que são mais inteligentes que os demais, pois os worns são auto replicantes, ou seja, ele cria varias copias de si mesmo e infecta outros computadores. Esta infeção pode acontecer por meio de conexões de rede local, pela internet ou anexos de e-mail.

O worn pode enviar copias de si próprio para todos os contatos de seu e-mail, e depois disso, os computadores destas pessoas farão o mesmo, causando um efeito de avalanche, com isso ocorrera o congestionamento de redes das empresas e da internet. Com esse congestionamento eles entopem as redes e podem criar grandes períodos de espera para abrir paginas na Internet.

**Spyware**

O Spyware são programas espiões, onde sua função é “espionar” as informações sobre uma ou mais atividades realizadas em um computador. Existem Spyware que são projetados para o mau e outros para o bem. Os Spyware maus são feitos para visualizar as atividades dos usuários e capturar informações sobre ele, onde posteriormente são transmitidos pela Internet, contendo desde hábitos de navegação do usuário até senhas. Os Spyware bons são usados por empresas de anuncio que se utilizam para de forma legal, coletar informações dos assinantes, com vistas a selecionar o tipo de anuncio que irão lhes apresentar.

**KeyLogger**

O KeyLogger são programas que são capazes de gravar tudo o que uma pessoa desavisada digitar no teclado, incluindo senhas de acesso a contas de banco, email, entre outros. Aplicativos com função keylogging foram criados com intuito de monitorar a atividades de funcionários de uma empresa e até para os pais saberem o que os filhos acessam na internet.

Na maioria das ocasiões, o KeyLogger é instalado no computador quando o usuario abre email ou conteúdos baixados da internet que continham o programa disfarçado entre os arquivos. Essa ferramenta já foi responsável por vários roubos milionários em contas bancarias, especialmente no Brasil.

**Hijacker**

São programas que “sequestram” navegadores de internet. Eles entram em seu computador e modificam os registros do Windows, assim eles conseguem modificar a pagina inicial dele e impedir que seja mudado, exibir anúncios em janelas novas, instalar barras de ferramentas e bloquear o acesso a determinados sites. Todas as coisas que são alteradas em seu navegador, geralmente linkam para publicidade, e quem saem ganhando com isso, é o próprio desenvolvedor do Hijack, pois ele é pago cada vez que esta publicidade é aberta.

**Ransomware**

São malware criado com o intuito de bloquear ou limitar o acesso a arquivos, pastas, aplicativos, unidades de armazenamento inteiras ou até mesmo impedir o uso do sistema Operacional. Para liberar esses recursos, o ransomware costuma mostrar mensagens exigindo pagamentos.

Para convencer o usuário a desembolsar o valor exigido, a mensagem pode conter ameaças ou chantagens, dizendo que dados importantes serão apagados ou que imagens particulares da pessoa serão publicadas na internet caso o pagamento não seja efetuado.