1.*Memory Injections*

Todo software que roda em um computador precisa ser carregado na memória antes de ser executado pelo processador. Isso inclui tanto programas legítimos quanto malware, que deve encontrar uma maneira de se infiltrar na memória para operar. Dentro da memória, existem diversos processos em execução simultânea, incluindo bibliotecas dinâmicas (DLLs), threads e buffers que fazem parte do gerenciamento do sistema. Para executar seu código malicioso, o malware pode optar por rodar como um processo independente ou se injetar dentro de um processo legítimo já em execução.

A injeção de malware em um processo existente pode trazer diversas vantagens para o atacante. Além de evitar a detecção por programas antivírus que monitoram processos suspeitos, essa técnica também permite que o malware herde os mesmos privilégios e permissões do processo original. Dessa forma, se o processo alvo possuir acesso administrativo ao sistema, o código injetado também terá, possibilitando uma elevação de privilégios sem chamar a atenção da segurança.

Uma das formas mais comuns de injeção de malware é chamada de **DLL Injection**, que explora o funcionamento das **Dynamic-Link Libraries (DLLs)** no Windows. As DLLs são arquivos executáveis que podem ser compartilhados entre diferentes programas, permitindo que múltiplas aplicações utilizem os mesmos recursos sem duplicação desnecessária de código. Para que essa técnica funcione, o atacante primeiro precisa armazenar a DLL maliciosa em algum local acessível pelo sistema. Em seguida, ele configura um caminho para esse arquivo dentro de um processo legítimo em execução.

Quando esse processo precisar carregar uma biblioteca DLL, ele consultará o caminho indicado e carregará o arquivo malicioso na memória, permitindo que o código do atacante seja executado sem despertar suspeitas. Como o processo original já possui privilégios no sistema, o malware injetado pode operar com os mesmos direitos, dificultando sua detecção e remoção. Essa técnica é amplamente utilizada por criminosos para manter acesso persistente a sistemas comprometidos e executar ações maliciosas sem chamar a atenção de mecanismos de segurança.