Técnicas Mitre Abordadas

Técnicas Mitre	Resumo	Cenários de Treinamento
T1037	Malware pode instruir o Windows a executar scripts maliciosos na inicialização ou quando um usuário efetua login.	
T1055	Injeção de processo, geralmente usada para executar código malicioso em um processo alvo, permitindo que o processo original continue.	Cenário de Treinamento - Injeção de Processo
T1055-001	A injeção de DLL pode ser usada para carregar código malicioso em um processo simplesmente instruindo o processo alvo a carregar uma nova DLL ou substituindo uma DLL legítima antes que ela seja carregada.	Cenário de Treinamento - Injeção de DLL
T1055-005	Injeção de processo por modificação do armazenamento local de thread, enganando a aplicação para executar código malicioso durante o gerenciamento de threads.	
T1055-012	Injeção de processo por substituição de código em um processo, tipicamente antes de sua execução começar.	Cenário de Treinamento - Modificação de Memória
T1055-013	Injeção de processo executando um executável malicioso enquanto engana o sistema operacional e os produtos de segurança para que analisem uma versão mais antiga do executável.	
T1059-001	O PowerShell é frequentemente usado por malware do Windows para realizar a configuração do malware, como substituir arquivos legítimos por maliciosos.	
T1068	A execução de escalonamento de privilégios por meio de vulnerabilidades de software pode permitir que código malicioso escape de restrições de permissão ou de ambientes virtualizados.	

T1091	O malware pode se replicar em mídias removíveis para que a próxima máquina a conectá-la possa executá-lo via execução automática ou vulnerabilidades de drivers.	
T1106	As APIs nativas costumam ser o acesso mais direto à funcionalidade do sistema operacional para acessar arquivos, executar processos e muito mais.	
T1204	A execução pelo usuário, frequentemente obtida por meio de phishing, é a forma mais simples de o malware começar a ser executado.	Cenário de Treinamento - Ransomware Básico
T1212	Credenciais podem ser roubadas ao se aproveitar de software vulnerável que não criptografa as credenciais inseridas por um usuário.	Cenário de Treinamento - Roubo de Identidade Cenário de Treinamento - Enumeração de Dados
T1543	Criar ou modificar um processo do sistema pode disfarçar código malicioso como um processo normal e confiável do sistema, evitando a detecção de malware.	Cenário de Treinamento - Injeção de Processo Cenário de Treinamento - Modificação de Memória
T1547	O malware pode instruir o Windows a executar programas maliciosos na inicialização ou quando um usuário efetua login.	
T1548	Abusar do controle de elevação pode permitir que um processo que normalmente não teria privilégios mais altos seja escalonado para obter acesso a dados protegidos.	
T1555	Credenciais armazenadas em gerenciadores ou navegadores não criptografados podem ser usadas para obter acesso a dados privilegiados.	Cenário de Treinamento - Roubo de Identidade
T1559	A comunicação entre processos pode fornecer controle sobre o processo alvo a partir do injetor, uma vez concluída a injeção.	Cenário de Treinamento - Injeção de Processo Cenário de Treinamento - Injeção de DLL Cenário de Treinamento - Modificação de Memória

T1566	O phishing pode ser usado para enganar um usuário a realizar uma ação que ele não teria feito de outra forma, como executar um script ou compartilhar uma senha.	Cenário de Treinamento - Ransomware Básico
T1569	Injetar em um serviço do sistema, como um `svchost` existente, pode disfarçar código malicioso para que seja reportado como sendo executado a partir de um processo bem conhecido e confiável.	Cenário de Treinamento - Injeção de Processo
T1574-002	DLLs maliciosas podem ser forçadas a carregar em um processo que, de outra forma, seria legítimo.	Cenário de Treinamento - Injeção de DLL
T1574-007	Recursos executáveis como DLLs podem ser redirecionados para substitutos maliciosos ao se abusar da variável de ambiente `PATH`.	Cenário de Treinamento - Injeção de DLL
T1587-002	Certificados de assinatura de código são uma forma de uma autoridade certificar o código de uma aplicação. O malware pode gerar um certificado que não vem de nenhuma autoridade certificadora, mas pode confundir um usuário fazendo-o pensar que é legítimo.	Cenário de Treinamento - Ransomware Assinado
T1587-003	Os certificados SSL são usados para garantir que a transmissão de dados seja confiável. Em um ambiente mal configurado, o malware pode conseguir instalar seu próprio certificado SSL para facilitar ataques do tipo man in the middle.	Cenário de Treinamento - Ransomware Assinado

Revision #1
Created 2026-07-24 05:10:41 UTC by Dennis Underwood
Updated 2026-07-24 05:10:41 UTC by Dennis Underwood