Técnicas de Mitre Cubiertas

Técnicas Mitre	Resumen	Escenarios de Capacitación
T1037	El malware puede indicar a Windows que ejecute scripts maliciosos durante el arranque o cuando un usuario inicia sesión.	
T1055	Inyección de procesos, generalmente utilizada para ejecutar código malicioso dentro de un proceso objetivo mientras se permite que el proceso original continúe.	Escenario de Capacitación - Inyección de Procesos
T1055-001	La inyección de DLL se puede utilizar para cargar código malicioso en un proceso simplemente indicando al proceso objetivo que cargue una nueva DLL o reemplazando una DLL legítima antes de que se cargue.	Escenario de Capacitación - Inyección de DLL
T1055-005	Inyección de procesos mediante la modificación del almacenamiento local de subprocesos, engañando a la aplicación para que ejecute código malicioso durante la gestión de subprocesos.	
T1055-012	Inyección de procesos mediante el reemplazo de código en un proceso, generalmente antes de que comience su ejecución.	Escenario de Capacitación - Modificación de Memoria
T1055-013	Inyección de procesos mediante la ejecución de un ejecutable malicioso mientras se engaña al sistema operativo y a los productos de seguridad para que analicen una versión anterior del ejecutable.	
T1059-001	PowerShell es utilizado frecuentemente por el malware de Windows para realizar la configuración del malware, como reemplazar archivos legítimos por archivos maliciosos.	
T1068	Realizar la escalada de privilegios mediante vulnerabilidades de software puede permitir que el código malicioso evada restricciones de permisos o entornos virtualizados.	

T1091	El malware puede replicarse a sí mismo en medios extraíbles para que la siguiente máquina que los conecte pueda ejecutarlo mediante autorun o vulnerabilidades de controladores.	
T1106	Las API nativas suelen ser el acceso más cercano a la funcionalidad del sistema operativo para acceder a archivos, ejecutar procesos y más.	
T1204	La ejecución por parte del usuario, a menudo obtenida mediante phishing, es la forma más simple en que el malware puede comenzar a ejecutarse.	Escenario de Capacitación - Ransomware Estándar
T1212	Las credenciales podrían ser robadas aprovechando software vulnerable que no cifra las credenciales introducidas por un usuario.	Escenario de Capacitación - Robo de Identidad Escenario de Capacitación - Enumeración de Datos
T1543	Crear o modificar un proceso del sistema puede disfrazar el código malicioso como un proceso del sistema normal y confiable, evadiendo la detección de malware.	Escenario de Capacitación - Inyección de Procesos Escenario de Capacitación - Modificación de Memoria
T1547	El malware puede indicar a Windows que ejecute programas maliciosos durante el arranque o cuando un usuario inicia sesión.	
T1548	El abuso del control de elevación puede permitir que un proceso que normalmente no tendría privilegios elevados sea escalado para obtener acceso a datos protegidos.	
T1555	Las credenciales almacenadas en gestores o navegadores sin cifrar pueden utilizarse para obtener acceso a datos privilegiados.	Escenario de Capacitación - Robo de Identidad
T1559	La comunicación entre procesos puede proporcionar control sobre el proceso objetivo por parte del inyector una vez que la inyección se ha completado.	Escenario de Capacitación - Inyección de Procesos Escenario de Capacitación - Inyección de DLL Escenario de Capacitación - Modificación de Memoria

T1566	El phishing puede utilizarse para engañar a un usuario y hacer que realice una acción que de otro modo no hubiera realizado, como ejecutar un script o compartir una contraseña.	Escenario de Capacitación - Ransomware Estándar
T1569	La inyección en un servicio del sistema como un `svchost` existente puede disfrazar el código malicioso para que se reporte como ejecutándose desde un proceso conocido y confiable.	Escenario de Capacitación - Inyección de Procesos
T1574-002	Se puede forzar la carga de DLL maliciosas en un proceso que de otro modo sería legítimo.	Escenario de Capacitación - Inyección de DLL
T1574-007	Los recursos ejecutables como las DLL pueden redirigirse a sustitutos maliciosos abusando de la variable de entorno `PATH`.	Escenario de Capacitación - Inyección de DLL
T1587-002	Los certificados de firma de código son una forma en que una autoridad certifica el código de una aplicación. El malware puede generar un certificado que no proviene de ninguna autoridad certificadora, pero que puede confundir a un usuario haciéndole creer que es legítimo.	Escenario de Capacitación - Ransomware Firmado
T1587-003	Los certificados SSL se utilizan para garantizar que la transmisión de datos sea confiable. En un entorno mal configurado, el malware puede ser capaz de instalar su propio certificado SSL para facilitar ataques de intermediario (man in the middle).	Escenario de Capacitación - Ransomware Firmado

Revision #1
Created 2026-07-24 01:12:27 UTC by Dennis Underwood
Updated 2026-07-24 01:12:27 UTC by Dennis Underwood