Mitre Techniques Covered

Created by Noah Greenberg, last modified on Nov 03, 2022

Mitre Techniques	Summary	Training Scenarios
T1037	Malware may instruct Windows to execute malicious scripts on boot or when a user logs in.	
T1055	Process injection, usually used to run malicious code in a target process while allowing the original process to continue.	Training Scenario - Process Injection
T1055-001	DLL injection can be used to load malicious code into a process by simply instructing the target process to load a new DLL or by replacing a legitimate DLL before it is loaded.	Training Scenario - DLL Injection
T1055-005	Process injection by modification of thread local storage, tricking the application into running malicious code during thread management.	
T1055-012	Process injection by replacing code in a process, typically before it begins execution.	Training Scenario - Memory Modification
T1055-013	Process injection by executing a malicious executable while tricking the OS and security products into scanning an older revision of the executable.	
T1059-001	PowerShell is often used by Windows malware to perform malware setup, such as replacing legitimate files with malicious ones.	
T1068	Performing privilege escalation via software vulnerabilities can allow malicious code to escape permission restrictions or virtualized environments.	
T1091	Malware may replicate itself onto removable media so that the next machine to connect it may execute via autorun or driver vulnerabilities.	

T1106	Native APIs are often the closest access to operating system functionality for accessing files, running processes, and more.	
T1204	User execution, often gained via phishing, is the simplest way malware may begin running.	Training Scenario - Vanilla Ransomware
T1212	Credentials could be stolen by taking advantage of vulnerable software that does not encrypt credentials inputted by a user.	Training Scenario - Identity Theft Training Scenario - Data Enumeration
T1543	Creating or modifying a system process can disguise malicious code as a normal, trusted system process from malware detection.	Training Scenario - Process Injection Training Scenario - Memory Modification
T1547	Malware may instruct Windows to execute malicious programs on boot or when a user logs in.	
T1548	Abusing elevation control can allow a process that would not normally have higher privileges be escalated to gain access to protected data.	
T1555	Stored credentials from unencrypted managers or browsers may be used to gain access to privileged data.	Training Scenario - Identity Theft
T1559	Inter-Process communication can provide control over the target process from the injector once the injection is complete.	Training Scenario - Process Injection Training Scenario - DLL Injection Training Scenario - Memory Modification
T1566	Phishing may be used to trick a user into performing an action they would not have done otherwise such as running a script or sharing a password.	Training Scenario - Vanilla Ransomware
T1569	Injecting into a system service such as an existing `svchost` can disguise malicious code to be reported as running from a well known and trusted process.	Training Scenario - Process Injection
T1574-002	Malicious DLLs can be forced to load into an otherwise legitimate process.	Training Scenario - DLL Injection
T1574-007	Executable resources such as DLLs can be redirected to malicious substitutes by abusing the `PATH` environment variable.	Training Scenario - DLL Injection

T1587-002	Code signing certificates are a way for an authority to certify that an applications code. Malware may generate a certificate that does not come from any certificate authority but may confuse a user into thinking it is legitimate.	Training Scenario - Signed Ransomware
T1587-003	SSL certificates are used to ensure that data transmission is trustworthy. In a poorly configured environment, malware may be able to install its own SSL certificate to facilitate man in the middle attacks.	Training Scenario - Signed Ransomware

Revision #1
Created 2026-05-18 20:29:20 UTC by Dennis Underwood
Updated 2026-05-18 20:29:20 UTC by Dennis Underwood