Abgedeckte Mitre-Techniken

Mitre-Techniken	Zusammenfassung	Trainingsszenarien
T1037	Malware kann Windows anweisen, bösartige Skripte beim Start oder bei der Anmeldung eines Benutzers auszuführen.	
T1055	Prozessinjektion, üblicherweise verwendet, um bösartigen Code in einem Zielprozess auszuführen, während der ursprüngliche Prozess weiterlaufen kann.	Trainingsszenario - Prozessinjektion
T1055-001	DLL-Injektion kann verwendet werden, um bösartigen Code in einen Prozess zu laden, indem der Zielprozess einfach angewiesen wird, eine neue DLL zu laden, oder indem eine legitime DLL vor dem Laden ersetzt wird.	Trainingsszenario - DLL-Injektion
T1055-005	Prozessinjektion durch Modifikation des Thread Local Storage, wodurch die Anwendung dazu gebracht wird, während der Thread-Verwaltung bösartigen Code auszuführen.	
T1055-012	Prozessinjektion durch Ersetzen von Code in einem Prozess, typischerweise bevor dieser mit der Ausführung beginnt.	Trainingsszenario - Speichermodifikation
T1055-013	Prozessinjektion durch Ausführung einer bösartigen ausführbaren Datei, während das Betriebssystem und Sicherheitsprodukte dazu gebracht werden, eine ältere Version der ausführbaren Datei zu scannen.	
T1059-001	PowerShell wird von Windows-Malware häufig verwendet, um die Malware-Einrichtung durchzuführen, z. B. das Ersetzen legitimer Dateien durch bösartige.	

T1068	Die Durchführung einer Rechteausweitung über Softwareschwachstellen kann es bösartigem Code ermöglichen, Berechtigungseinschränkungen oder virtualisierte Umgebungen zu umgehen.	
T1091	Malware kann sich selbst auf Wechseldatenträger kopieren, sodass sie beim Anschließen an den nächsten Rechner über Autorun oder Treiberschwachstellen ausgeführt werden kann.	
T1106	Native APIs bieten oft den direktesten Zugriff auf Betriebssystemfunktionen zum Zugriff auf Dateien, zum Ausführen von Prozessen und mehr.	
T1204	Die Ausführung durch den Benutzer, häufig durch Phishing erreicht, ist der einfachste Weg, wie Malware zu laufen beginnen kann.	Trainingsszenario - Vanilla-Ransomware
T1212	Anmeldedaten könnten gestohlen werden, indem eine verwundbare Software ausgenutzt wird, die vom Benutzer eingegebene Anmeldedaten nicht verschlüsselt.	Trainingsszenario - Identitätsdiebstahl Trainingsszenario - Datenenumeration
T1543	Das Erstellen oder Modifizieren eines Systemprozesses kann bösartigen Code als normalen, vertrauenswürdigen Systemprozess vor der Malware-Erkennung tarnen.	Trainingsszenario - Prozessinjektion Trainingsszenario - Speichermodifikation
T1547	Malware kann Windows anweisen, bösartige Programme beim Start oder bei der Anmeldung eines Benutzers auszuführen.	
T1548	Der Missbrauch der Rechteerhöhung kann dazu führen, dass ein Prozess, der normalerweise keine höheren Berechtigungen hätte, erweitert wird, um Zugriff auf geschützte Daten zu erlangen.	
T1555	Gespeicherte Anmeldedaten aus unverschlüsselten Managern oder Browsern können verwendet werden, um Zugriff auf privilegierte Daten zu erlangen.	Trainingsszenario - Identitätsdiebstahl

T1559	Interprozesskommunikation kann dem Injektor die Kontrolle über den Zielprozess ermöglichen, sobald die Injektion abgeschlossen ist.	Trainingsszenario - Prozessinjektion Trainingsszenario - DLL-Injektion Trainingsszenario - Speichermodifikation
T1566	Phishing kann verwendet werden, um einen Benutzer dazu zu bringen, eine Handlung auszuführen, die er sonst nicht getan hätte, wie z. B. das Ausführen eines Skripts oder das Teilen eines Passworts.	Trainingsszenario - Vanilla-Ransomware
T1569	Die Injektion in einen Systemdienst wie einen bestehenden `svchost` kann bösartigen Code so tarnen, dass er als von einem bekannten und vertrauenswürdigen Prozess ausgehend gemeldet wird.	Trainingsszenario - Prozessinjektion
T1574-002	Bösartige DLLs können gezwungen werden, in einen ansonsten legitimen Prozess geladen zu werden.	Trainingsszenario - DLL-Injektion
T1574-007	Ausführbare Ressourcen wie DLLs können durch Missbrauch der Umgebungsvariable `PATH` auf bösartige Ersatzdateien umgeleitet werden.	Trainingsszenario - DLL-Injektion
T1587-002	Code-Signaturzertifikate sind eine Möglichkeit für eine Autorität, den Code einer Anwendung zu zertifizieren. Malware kann ein Zertifikat erzeugen, das von keiner Zertifizierungsstelle stammt, aber einen Benutzer glauben machen kann, es sei legitim.	Trainingsszenario - Signierte Ransomware
T1587-003	SSL-Zertifikate werden verwendet, um sicherzustellen, dass die Datenübertragung vertrauenswürdig ist. In einer schlecht konfigurierten Umgebung kann Malware in der Lage sein, ihr eigenes SSL-Zertifikat zu installieren, um Man-in-the-Middle-Angriffe zu ermöglichen.	Trainingsszenario - Signierte Ransomware

Revision #1
Created 2026-07-24 03:53:32 UTC by Dennis Underwood
Updated 2026-07-24 03:53:32 UTC by Dennis Underwood