Techniques Mitre couvertes

Techniques Mitre	Résumé	Scénarios de formation
T1037	Un logiciel malveillant peut demander à Windows d'exécuter des scripts malveillants au démarrage ou lors de la connexion d'un utilisateur.	
T1055	Injection de processus, généralement utilisée pour exécuter du code malveillant dans un processus cible tout en permettant au processus d'origine de continuer.	Training Scenario - Process Injection
T1055-001	L'injection de DLL peut être utilisée pour charger du code malveillant dans un processus en demandant simplement au processus cible de charger une nouvelle DLL ou en remplaçant une DLL légitime avant son chargement.	Training Scenario - DLL Injection
T1055-005	Injection de processus par modification du stockage local des threads (thread local storage), incitant l'application à exécuter du code malveillant lors de la gestion des threads.	
T1055-012	Injection de processus par remplacement de code dans un processus, généralement avant le début de son exécution.	Training Scenario - Memory Modification
T1055-013	Injection de processus par exécution d'un exécutable malveillant tout en trompant le système d'exploitation et les produits de sécurité en leur faisant analyser une révision antérieure de l'exécutable.	
T1059-001	PowerShell est souvent utilisé par les logiciels malveillants Windows pour effectuer l'installation du malware, comme le remplacement de fichiers légitimes par des fichiers malveillants.	

T1068	L'élévation de privilèges via des vulnérabilités logicielles peut permettre à du code malveillant d'échapper aux restrictions de permissions ou aux environnements virtualisés.	
T1091	Un logiciel malveillant peut se répliquer sur un support amovible afin que la prochaine machine sur laquelle il est connecté puisse l'exécuter via l'exécution automatique ou des vulnérabilités de pilotes.	
T1106	Les API natives constituent souvent l'accès le plus direct aux fonctionnalités du système d'exploitation pour l'accès aux fichiers, l'exécution de processus, et bien plus encore.	
T1204	L'exécution par l'utilisateur, souvent obtenue via le phishing, est la manière la plus simple pour un logiciel malveillant de commencer à s'exécuter.	Training Scenario - Vanilla Ransomware
T1212	Des identifiants peuvent être volés en exploitant un logiciel vulnérable qui ne chiffre pas les identifiants saisis par un utilisateur.	Training Scenario - Identity Theft Training Scenario - Data Enumeration
T1543	La création ou la modification d'un processus système peut déguiser du code malveillant en un processus système normal et de confiance afin d'échapper à la détection de logiciels malveillants.	Training Scenario - Process Injection Training Scenario - Memory Modification
T1547	Un logiciel malveillant peut demander à Windows d'exécuter des programmes malveillants au démarrage ou lors de la connexion d'un utilisateur.	
T1548	Le détournement du contrôle d'élévation peut permettre à un processus qui n'aurait normalement pas de privilèges plus élevés d'être élevé afin d'accéder à des données protégées.	
T1555	Des identifiants stockés provenant de gestionnaires ou de navigateurs non chiffrés peuvent être utilisés pour accéder à des données privilégiées.	Training Scenario - Identity Theft

T1559	La communication inter-processus peut fournir un contrôle sur le processus cible à partir de l'injecteur une fois l'injection terminée.	Training Scenario - Process Injection Training Scenario - DLL Injection Training Scenario - Memory Modification
T1566	Le phishing peut être utilisé pour inciter un utilisateur à effectuer une action qu'il n'aurait pas effectuée autrement, comme exécuter un script ou partager un mot de passe.	Training Scenario - Vanilla Ransomware
T1569	L'injection dans un service système tel qu'un `svchost` existant peut déguiser du code malveillant afin qu'il soit signalé comme provenant d'un processus bien connu et de confiance.	Training Scenario - Process Injection
T1574-002	Des DLL malveillantes peuvent être forcées à se charger dans un processus par ailleurs légitime.	Training Scenario - DLL Injection
T1574-007	Des ressources exécutables telles que des DLL peuvent être redirigées vers des substituts malveillants en exploitant la variable d'environnement `PATH`.	Training Scenario - DLL Injection
T1587-002	Les certificats de signature de code sont un moyen pour une autorité de certifier le code d'une application. Un logiciel malveillant peut générer un certificat qui ne provient d'aucune autorité de certification, mais qui peut induire un utilisateur en erreur en lui faisant croire qu'il est légitime.	Training Scenario - Signed Ransomware
T1587-003	Les certificats SSL sont utilisés pour garantir que la transmission des données est fiable. Dans un environnement mal configuré, un logiciel malveillant peut être en mesure d'installer son propre certificat SSL pour faciliter les attaques de type man in the middle.	Training Scenario - Signed Ransomware

Revision #1
Created 2026-07-24 06:18:49 UTC by Dennis Underwood
Updated 2026-07-24 06:18:49 UTC by Dennis Underwood