AYI NEDJIMI Consultants

MITRE ATT&CK : Les 10 Techniques les Plus Utilisées en

Catégorie : Techniques de Hacking Lecture : 9 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Analyse des 10 techniques MITRE ATT&CK les plus observées en 2026 : Process Injection T1055, Defense Evasion, Credential Access. Détection, hunting.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

La technique d'injection de processus occupe la première place de notre classement, et ce n'est pas une surprise. **T1055 Process Injection** est la pierre angulaire de l'arsenal offensif moderne. Elle permet à un attaquant d'exécuter du code arbitraire dans l'espace mémoire d'un processus légitime, obtenant ainsi à la fois l'évasion des défenses (le code malveillant s'exécute sous l'identité d'un processus de confiance) et une élévation de privilèges potentielle. Analyse des 10 techniques MITRE ATT&CK les plus observées en 2026 : Process Injection T1055, Defense Evasion, Credential Access. Détection, hunting. Les techniques offensives évoluent rapidement : mitre attck top techniques 2026 fait partie des compétences essentielles que tout pentester et red teamer doit maîtriser pour mener des missions réalistes. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Les variantes principales (T1055.001 à T1055.012)

ATT&CK recense douze sous-techniques de Process Injection, chacune exploitant un mécanisme spécifique du système d'exploitation :

DLL Injection (T1055.001)

La méthode la plus classique. L'attaquant force un processus cible à charger une DLL malveillante via `CreateRemoteThread` combiné à `LoadLibrary`. Bien que ancienne, cette technique reste efficace car de nombreuses applications légitimes chargent des DLL dynamiquement, rendant le comportement difficile à distinguer du fonctionnement normal. Les outils comme Cobalt Strike, Havoc et Sliver l'implémentent nativement.

Process Hollowing (T1055.012)

Technique plus complexe : l'attaquant crée un processus légitime en état suspendu (par exemple `svchost.exe`), vide son contenu mémoire via `NtUnmapViewOfSection`, puis injecte son propre code avant de reprendre l'exécution. Le processus apparaît légitime dans le gestionnaire de tâches et les outils de monitoring classiques. Le Process Hollowing est particulièrement prisé par les groupes de ransomware comme LockBit et BlackCat/ALPHV car il permet de contourner les listes blanches d'applications.

APC Injection (T1055.004)
L'injection via Asynchronous Procedure Call exploite le mécanisme APC de Windows pour forcer un thread cible à exécuter du code lors de son prochain état d'alerte (alertable state). La variante "Early Bird" injecte le code avant même que le processus n'ait terminé son initialisation, contournant ainsi les hooks EDR posés au démarrage du processus. Cette technique est devenue un standard dans les implants APT depuis les campagnes de APT29 (Cozy Bear) et est largement documentée dans les analyses de techniques d'évasion EDR.

Thread Execution Hijacking (T1055.003)
Notre avis d'expert
La divulgation responsable des vulnérabilités est un pilier de la sécurité collective. Trop d'entreprises traitent encore les chercheurs en sécurité comme des menaces plutôt que des alliés. Un programme de bug bounty bien structuré peut transformer cette dynamique.

Vos équipes savent-elles réagir face à une intrusion en cours ?

L'attaquant suspend un thread existant d'un processus légitime, modifie son contexte d'exécution (registre EIP/RIP) pour pointer vers le shellcode injecté, puis reprend le thread. Cette technique ne crée pas de nouveau thread, ce qui la rend particulièrement furtive face aux EDR qui surveillent les appels `CreateRemoteThread`.

NTDLL Unhooking
Bien que pas directement une sous-technique T1055, le NTDLL unhooking est devenu indissociable de l'injection de processus moderne. Les EDR placent des hooks (détours) dans les fonctions critiques de `ntdll.dll` pour intercepter les appels système. Les attaquants contournent ces hooks en rechargeant une copie "propre" de ntdll depuis le disque ou directement depuis les syscalls, rendant les injections invisibles. Les frameworks comme SysWhispers3 et HellsGate automatisent ce contournement.

Extra Window Memory Injection (T1055.011)
Cette variante exploite les structures de fenêtres Windows (Extra Window Memory) pour stocker et exécuter du shellcode. Utilisée notamment par le malware PowerLoader et certaines variantes de Dridex, elle reste peu connue des analystes SOC et donc rarement détectée.

Stratégies de détection pour T1055

- **Sysmon Event ID 8** (CreateRemoteThread) : surveiller les créations de threads inter-processus, en particulier lorsque le processus source n'est pas un parent légitime du processus cible.
- **Sysmon Event ID 10** (ProcessAccess) : détecter les accès mémoire suspects avec les flags `PROCESS_VM_WRITE` et `PROCESS_VM_OPERATION`.
- **ETW (Event Tracing for Windows)** : les providers Microsoft-Windows-Threat-Intelligence et Microsoft-Windows-Kernel-Process fournissent une télémétrie granulaire sur les opérations mémoire.
- **Memory scanning** : les outils comme PE-sieve, Moneta et YARA permettent de détecter les régions mémoire RWX (Read-Write-Execute) suspectes et les PE non mappés en mémoire.
- **Analyse comportementale** : un processus `svchost.exe` qui effectue des connexions réseau inhabituelles ou un `notepad.exe` qui charge `ws2_32.dll` sont des indicateurs forts.

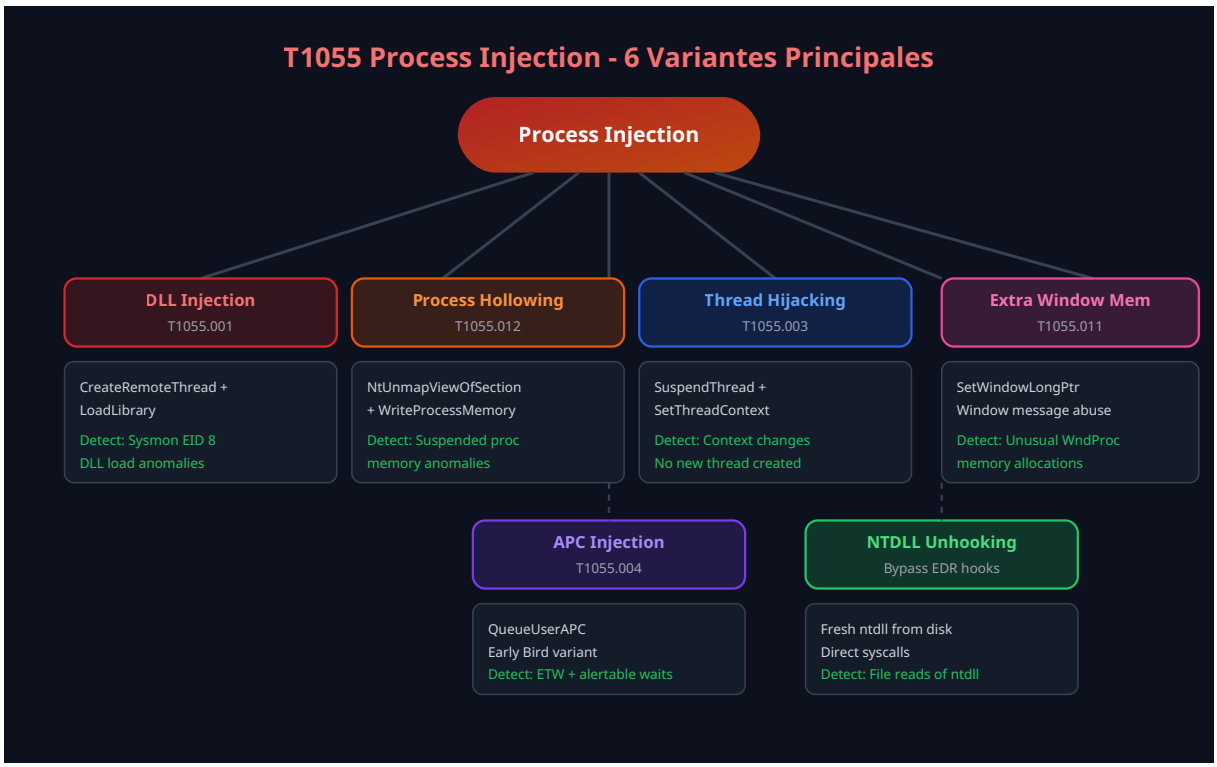

Figure 1 : Les 6 variantes principales de Process Injection (T1055) avec leurs API caractéristiques et indicateurs de détection

Windows Credential Manager et Windows Vault stockent les credentials pour les connexions réseau, les sessions RDP et les applications. L'abus de DPAPI est devenu un axe majeur d'attaque : un attaquant disposant du hash NTLM d'un utilisateur ou des clés de sauvegarde DPAPI du domaine peut déchiffrer hors ligne tous les secrets protégés par DPAPI, y compris les credentials Wi-Fi, les certificats et les cookies de session. Le module `sekurlsa::dpapi` de Mimikatz et l'outil SharpDPAPI de GhostPack permettent cette extraction à grande échelle lors d'opérations de post-exploitation.

Accès à LSASS et extraction mémoire

Bien que techniquement distinct (T1003.001 LSASS Memory), l'accès au processus LSASS est souvent combiné avec T1555 dans les chaînes d'attaque réelles. Les méthodes modernes incluent le dump via `comsvcs.dll` (MiniDump), les outils comme Nanodump, PPLdump pour contourner la protection PPL (Protected Process Light), et même l'utilisation de pilotes vulnérables signés (BYOVD - Bring Your Own Vulnerable Driver) pour désactiver la protection PPL avant le dump. L'exploitation de Kerberos et le vol de TGT/TGS sont également liés à cette technique.

Stratégies de détection pour T1555

- **Monitoring d'accès fichiers** : surveiller les accès au fichier `Login Data` de Chrome, `key3.db` / `key4.db` de Firefox, et aux fichiers Vault de Windows Credential Manager par des processus non-navigateurs.
- **Protection LSASS** : activer Credential Guard, configurer LSASS en mode PPL (Protected Process Light), et surveiller les Event ID 4656/4663 pour les accès au processus lsass.exe.

- **Détection DPAPI** : surveiller les appels à `CryptUnprotectData` depuis des processus inhabituels et les accès aux Master Keys DPAPI dans le profil utilisateur.
- **Règles YARA** : déployer des signatures en mémoire pour Mimikatz, LaZagne et SharpDPAPI.

Quand avez-vous réalisé votre dernier test d'intrusion en conditions réelles ?

En 2026, les groupes de ransomware (en particulier les affiliés de RansomHub et Play) déploient systématiquement des instances portables de ScreenConnect ou AnyDesk comme canal d'accès persistant alternatif à leurs implants C2 traditionnels. Les attaques via le support technique frauduleux (Tech Support Scam) utilisent également ces outils pour prendre le contrôle des postes de travail des victimes après un appel téléphonique d'ingénierie sociale.

Détection clé pour T1219
Maintenir un inventaire strict des logiciels d'accès distant autorisés. Détecter les installations non approuvées via les Event ID 1 (Process Create) de Sysmon pour les binaires connus (anydesk.exe, teamviewer.exe, screenconnect*.exe). Bloquer les domaines de relay au niveau DNS/proxy pour les outils non autorisés. Surveiller les connexions réseau sortantes vers les infrastructures de relay connues.

#9 - Scheduled Task/Job (T1053)

T1053 couvre l'utilisation des planificateurs de tâches comme mécanisme de persistance, d'exécution et de mouvement latéral. Sur Windows, le Task Scheduler (`schtasks.exe`) permet de créer des tâches qui s'exécutent à des intervalles définis, au démarrage, ou en réponse à des événements. Sur Linux, `cron`, `at` et les timers systemd servent le même objectif.

En 2026, les attaquants utilisent des techniques d'évasion avancées pour les tâches planifiées : création de tâches avec des noms imitant des tâches système légitimes, utilisation de l'API COM pour créer des tâches sans passer par `schtasks.exe` (contournant ainsi les détections basées sur la ligne de commande), modification de tâches existantes plutôt que création de nouvelles, et utilisation de XML d'import pour des configurations complexes. Le mouvement latéral via les tâches planifiées distantes (`schtasks /create /s <remote_host>`) reste un classique des opérations de post-exploitation et pivoting.

Détection clé pour T1053
Surveiller les Event ID 4698 (task created) et 4702 (task updated) dans les logs Security. Utiliser Sysmon pour détecter les exécutions de schtasks.exe avec des arguments suspects. Baseline les tâches planifiées existantes et alerter sur toute déviation. Surveiller les créations de tâches distantes via l'analyse du trafic RPC/SMB.

Le mapping entre les sources de logs et les techniques ATT&CK est un exercice fondamental. Voici les correspondances clés pour notre top 10 :

Technique	Sources de logs primaires	Event IDs clés
T1055 Process Injection	Sysmon, ETW, EDR	Sysmon 8, 10, 25
T1555 Credential Stores	Sysmon, Security, EDR	Sysmon 1, 11; Security 4663
T1497 Sandbox Evasion	Sandbox logs, EDR	API calls (WMI, Registry)
T1071 App Layer Proto	Proxy, DNS, Zeek/NIDS	HTTP logs, DNS queries
T1036 Masquerading	Sysmon, EDR, AppLocker	Sysmon 1 (hash mismatch)
T1547 Boot Autostart	Sysmon, Security	Sysmon 12/13, Security 7045
T1562 Impair Defenses	Security, Sysmon, EDR health	Security 7040, Sysmon 6
T1219 Remote Access	Sysmon, Proxy, DNS	Sysmon 1, 3 (network)
T1053 Scheduled Task	Security, Sysmon, Task Scheduler	Security 4698/4702
T1027 Obfuscated Files	AMSI, Sysmon, EDR	AMSI events, Sysmon 7/15

Création de playbooks de chasse

Un playbook de chasse est un document structuré qui guide le hunter à travers une investigation spécifique. Pour chaque technique ATT&CK ciblée, le playbook doit inclure :

- **Contexte de la menace** : quels groupes utilisent cette technique, dans quels scénarios, et avec quels outils.
- **Prérequis en données** : quelles sources de logs doivent être collectées et dans quel niveau de détail (verbosité).
- **Requêtes de hunting** : requêtes Sigma, KQL, SPL ou EQL prêtes à l'emploi, avec des variantes pour différents niveaux de spécificité.
- **Procédure de triage** : arbre de décision pour qualifier les résultats (vrai positif, faux positif, nécessite investigation approfondie).
- **Actions de remédiation** : procédures à suivre en cas de découverte d'une compromission avérée.
- **Conversion en détection** : comment transformer le hunting en règle automatisée pour le SIEM/EDR.

Intégration SIEM : Splunk, Elastic, Sentinel

L'intégration d'ATT&CK dans les principales plateformes SIEM a considérablement mûri en 2026. **Splunk** offre le Content Pack ATT&CK avec des recherches préconfigurées mappées sur les techniques. **Elastic Security** intègre nativement le mapping ATT&CK dans ses règles de détection et son module de threat intelligence. **Microsoft Sentinel** propose des workbooks ATT&CK et des hunting queries alignées sur le framework. Le format **Sigma** permet d'écrire des règles de détection portables, convertibles automatiquement vers la syntaxe de chaque SIEM via sigmac ou pySigma.

```
# Exemple de règle Sigma pour détecter T1055 - Process Injection via CreateRemoteThread
title: Suspicious CreateRemoteThread - Process Injection
id: 66d31e5f-52d6-40a4-9615-002d3789a119
status: stable
description: Detects CreateRemoteThread calls to processes not typically targeted
logsource:
    category: create_remote_thread
    product: windows
detection:
    selection:
        SourceImage|endswith:
            - '\powershell.exe'
            - '\cmd.exe'
            - '\rundll32.exe'
            - '\regsvr32.exe'
    filter:
        TargetImage|endswith:
            - '\svchost.exe'
    condition: selection and not filter
level: high
tags:
    - attack.defense_evasion
    - attack.t1055
```

Atomic Red Team (projet Red Canary) fournit une bibliothèque de tests atomiques pour chaque technique ATT&CK, exécutables en une seule commande. Pour T1055.001 (DLL Injection), le test atomique injecte une DLL de test dans un processus cible et vérifie si la détection se déclenche. **MITRE Caldera** va plus loin en orchestrant des chaînes d'attaque complètes (opérations adversarial) simulant le comportement de groupes APT spécifiques. En 2026, Caldera 5.x intègre des plugins pour simuler plus de 400 techniques et sous-techniques avec un réalisme accru.

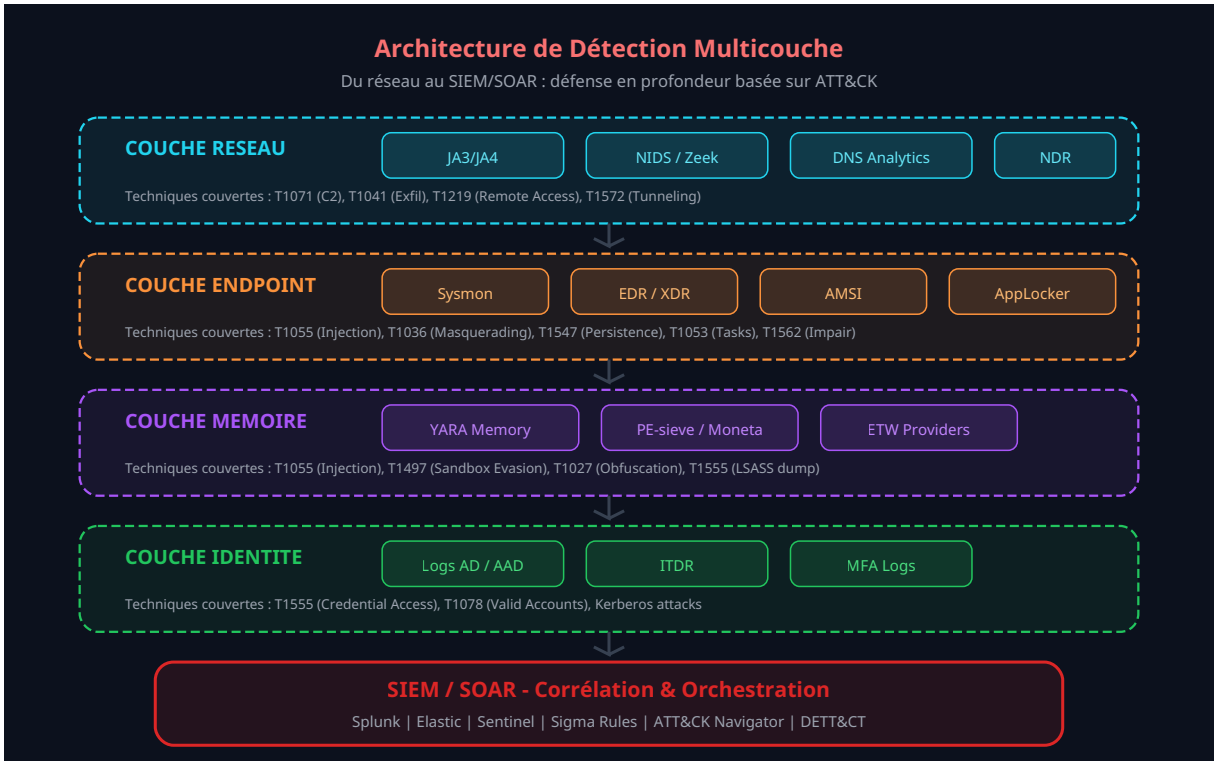

Figure 3 : Architecture de détection multicouche alignée sur les techniques ATT&CK - du réseau au SIEM/SOAR

Sources et références : MITRE ATT&CK · OWASP Testing Guide

FAQ

Qu'est-ce que MITRE ATT&CK ?

MITRE ATT&CK désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi mitre attck top techniques 2026 est-il important ?

La maîtrise de mitre attck top techniques 2026 est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

Conclusion

Le framework MITRE ATT&CK a transformé la manière dont les organisations abordent la cybersécurité défensive. En identifiant et en comprenant les dix techniques les plus utilisées par les attaquants en 2026, de l'injection de processus (T1055) à l'obfuscation de fichiers (T1027), les équipes de sécurité disposent d'une feuille de route claire pour prioriser leurs investissements en détection.

Les enseignements clés de cette analyse sont les suivants. Premièrement, la **défense en profondeur** reste indispensable : aucune couche de détection unique ne couvre l'ensemble des techniques. La combinaison de la surveillance réseau (JA3, NIDS), endpoint (Sysmon, EDR), mémoire (YARA, PE-sieve), identité (logs AD) et de la corrélation SIEM est nécessaire pour une couverture complète. Deuxièmement, le **threat hunting proactif** basé sur des hypothèses ATT&CK est le complément indispensable des détections automatisées. Troisièmement, la **validation continue** via des exercices Purple Team et des simulations Atomic Red Team/Caldera garantit que les détections fonctionnent réellement face aux techniques adverses actuelles.

La cybersécurité est une discipline dynamique : les techniques évoluent, de nouvelles sous-techniques apparaissent, et les outils défensifs doivent s'adapter continuellement. En ancrant votre stratégie défensive dans le framework ATT&CK, vous adoptez un langage commun qui facilite la communication entre équipes, la mesure de la maturité, et l'amélioration continue de votre posture de sécurité. L'objectif n'est pas de couvrir les 200+ techniques d'ATT&CK du jour au lendemain, mais de construire méthodiquement une couverture solide en commençant par les techniques les plus fréquemment observées, celles que cet article vous a présentées.

Références et ressources externes

- MITRE ATT&CK — Framework officiel de techniques et tactiques adverses

- ATT&CK Navigator — Outil de visualisation et de cartographie des couvertures
- Atomic Red Team — Bibliothèque de tests atomiques mappés sur ATT&CK
- MITRE Caldera — Plateforme de simulation d'adversaires automatisée
- DeTT&CT — Framework de suivi de couverture de détection
- SigmaHQ — Règles de détection génériques portables multi-SIEM

Points clés à retenir

- Les variantes principales (T1055.001 à T1055.012)
- Accès à LSASS et extraction mémoire
- #9 - Scheduled Task/Job (T1053)
- Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr