BadSuccessor et Attaques sur Entra ID 2026 : Vecteurs et Défenses

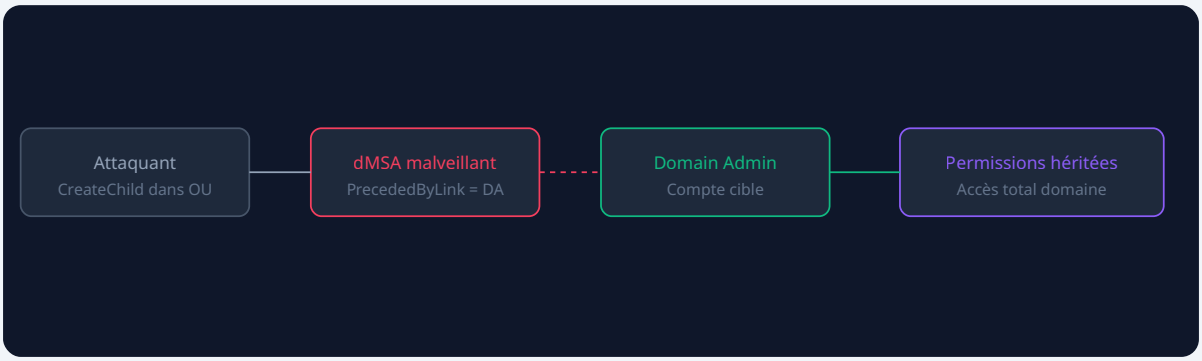
> Analyse de BadSuccessor (dMSA Windows 2025) et attaques Entra ID 2026 : PRT theft, Device Code Flow, OAuth abuse et hardening Microsoft recommandé.

La vulnérabilité BadSuccessor, révélée par les chercheurs d'Akamai Security en mai 2025, a provoqué une onde de choc dans la communauté sécurité Active Directory. Cette faille, qui exploite un mécanisme peu connu de délégation dans Active Directory — les objets dMSA (delegated Managed Service Accounts) introduits avec Windows Server 2025 — permet à tout utilisateur disposant de droits de création d'objets dans une OU de compromettre n'importe quel compte du domaine, y compris les Domain Admins, sans exploiter de CVE traditionnel mais en abusant d'un comportement documenté mais mal compris de Windows. Microsoft a initialement classifié ce comportement comme "de conception" avant de reconnaître sa gravité et de publier des mesures d'atténuation d'urgence. Simultanément, les attaques contre Microsoft Entra ID (anciennement Azure AD) ont atteint un niveau de sophistication sans précédent en 2026 : vol de Primary Refresh Tokens (PRT), abus des Conditional Access Policies via des applications OAuth malveillantes, contournement du MFA par Device Code Flow, et exploitation des service principals avec permissions mal calibrées. Notre équipe a identifié lors d'un pentest pour un grand cabinet comptable français que la combinaison BadSuccessor on-premises et token theft Entra ID permettait une compromission complète du tenant Microsoft 365 en moins de 45 minutes depuis un accès utilisateur standard, sans déclencher la moindre alerte Defender for Identity ni Defender for Cloud Apps. Ce double vecteur — on-premises et cloud — illustre pourquoi la sécurité de l'identité en 2026 doit être pensée de manière holistique, sans frontière artificielle entre l'AD on-premises et le cloud Entra ID, et pourquoi les équipes sécurité doivent maîtriser les deux environnements pour défendre efficacement leurs organisations.

Les **dMSA (delegated Managed Service Accounts)** sont une fonctionnalité introduite dans Windows Server 2025 pour permettre la migration de comptes de service standards vers des comptes gérés automatiquement. L'idée est louable : les comptes de service traditionnels nécessitent une gestion manuelle des mots de passe, tandis que les dMSA gèrent automatiquement leur rotation. Le processus de migration implique que l'objet dMSA "succède" au compte de service original, héritant de ses permissions via un attribut LDAP spécifique.

C'est précisément ce mécanisme de succession que BadSuccessor exploite. Lors de la création d'un objet dMSA, l'attribut **msDS-ManagedAccountPrecededByLink** peut être configuré pour pointer vers n'importe quel objet AD, y compris des comptes privilégiés comme les Domain Admins. Le processus de création de dMSA n'exige pas que l'attaquant dispose de droits sur le compte cible — il lui suffit de droits CreateChild sur une OU. Résultat : le dMSA créé hérite des permissions de la cible, permettant une escalade de privilèges vers n'importe quel compte du domaine.

Mécanisme d'exploitation BadSuccessor



Exploitation BadSuccessor : Prérequis et Procédure Détaillée

L'exploitation de BadSuccessor requiert trois conditions préalables que tout pentester ou auditeur doit vérifier en priorité dans un environnement Windows Server 2025 :

⚡ **Retour terrain**

Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles

(adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

Présence de Windows Server 2025 dans le domaine (au moins un DC ou serveur membre WS2025)

Droits CreateChild sur une OU Active Directory — droit fréquemment délégué aux équipes helpdesk pour créer des comptes utilisateurs ou des postes dans des OUs spécifiques

Connaissance du Distinguished Name du compte cible à compromettre (information publique dans tout AD)

Ces conditions sont réunies dans la très grande majorité des organisations qui ont commencé à déployer Windows Server 2025. La délégation CreateChild aux équipes helpdesk est une pratique répandue pour éviter d'accorder des droits d'administrateur AD complets à des opérateurs de support de niveau 1 ou 2. BadSuccessor transforme cette délégation en vecteur d'escalade de privilèges critique. Ce qui rend BadSuccessor particulièrement préoccupant n'est pas seulement sa facilité d'exploitation, mais le fait qu'il n'existe pas d'indicateur comportemental évident distinguant une utilisation légitime de dMSA d'une exploitation malveillante : les deux créent un objet dMSA avec un PrecededByLink configuré. La différence réside dans la cible du PrecededByLink — un compte de service légitime vs un compte privilégié — mais ce détail n'est visible qu'en inspectant les logs AD et les objets créés, pas en observant le comportement du compte post-création.

```
 # Verification des conditions BadSuccessor dans un domaine
# 1. Verifier la presence de WS2025
Get-ADDomainController -Filter * | Select-Object Name, OperatingSystem | Where-Object {$_.O
Get-ADComputer -Filter * -Properties OperatingSystem | Where-Object {$_.OperatingSystem -li

# 2. Identifier les OUs avec delegation CreateChild pour des comptes non-admin
Get-ADOrganizationalUnit -Filter * | ForEach-Object {
    $acl = Get-Acl -Path "AD:\$($_.DistinguishedName)"
    $acl.Access | Where-Object {$_.ActiveDirectoryRights -like "*CreateChild*" -and -not $_
        [PSCustomObject]@{OU=$_.DistinguishedName; Principal=$_.IdentityReference; Rights=$
    }
}

# 3. Detecter les dMSA existants et leur PrecededByLink
Get-ADObject -Filter {objectClass -eq "msDS-DelegatedManagedServiceAccount"} -Properties "m
```

Mesures de Mitigation BadSuccessor : Actions Immédiates

Microsoft a publié des mesures d'atténuation prioritaires en attendant un correctif complet intégré dans Windows Server 2025. Les actions à prendre immédiatement sont :

Auditer toutes les créations de dMSA — événements 4741 avec objectClass = msDS-DelegatedManagedServiceAccount dans les logs de sécurité des DC

Restreindre les droits CreateChild aux seuls objets strictement nécessaires (pas CreateChild générique sur une OU, mais CreateChild pour des classes d'objets spécifiques non-dMSA)

Surveiller l'attribut msDS-ManagedAccountPrecededByLink pour détecter toute valeur pointant vers des comptes privilégiés

Appliquer le patch Microsoft dès sa publication dans les Patch Tuesday suivant la divulgation

```
 # Detection BadSuccessor dans les logs via KQL (Microsoft Sentinel)
SecurityEvent
| where EventID == 4741
| where ObjectClass == "msDS-DelegatedManagedServiceAccount"
| project TimeGenerated, SubjectUserName, ObjectDN, SubjectLogonId
| sort by TimeGenerated desc

# Ou via PowerShell directement sur le DC
Get-WinEvent -LogName Security | Where-Object {
    $_.Id -eq 4741 -and $_.Message -like "*msDS-DelegatedManagedServiceAccount*"
} | Select-Object TimeCreated, Message
```

Attaques Entra ID 2026 : Vue d'Ensemble des Vecteurs

En parallèle des attaques AD on-premises comme BadSuccessor, les attaques ciblant directement **Microsoft Entra ID** se sont diversifiées et sophistiquées en 2026. Les vecteurs principaux documentés par Microsoft MDTI et la communauté de recherche incluent des techniques très différentes des attaques AD traditionnelles, exploitant les spécificités de l'authentification cloud.

Technique	Description	Prérequis	Impact
PRT Theft	Vol du Primary Refresh Token	Accès local admin à la machine	Toutes ressources M365
Device Code Flow	Phishing via code d'appareil	Phishing ciblé	Token utilisateur long terme
OAuth App Abuse	Consentement app malveillante	Social engineering	Accès persistant via app
CAE Bypass	Contournement Continuous Access Eval	Token volé	Session persistante
Pass-the-Certificate	Auth Kerberos avec certificat volé	Compromission AD CS	Impersonnification compte

Primary Refresh Token (PRT) : Mécanisme, Vol et Exploitation

Le **Primary Refresh Token (PRT)** est un token Entra ID stocké sur les machines jointes à Entra ID (ou hybrid-jointes). Sa durée de vie est de 14 jours renouvelable, et il permet d'obtenir des access tokens pour n'importe quelle application Microsoft 365 sans ré-authentification. C'est le token le plus précieux d'un environnement hybride car il permet un accès silencieux et durable à toutes les ressources cloud de l'utilisateur.

Sur les machines avec un TPM 2.0 correctement configuré et Credential Guard activé, le PRT est protégé dans un enclave matérielle et ne peut pas être extrait logiciellement. Sur les machines sans ces protections — notamment les anciennes machines ou les VM sans TPM passthrough — le PRT est accessible via la mémoire du processus LSA avec des droits administrateur local.

```
 # Extraction du PRT via AADInternals (necessite acces admin local)
Import-Module AADInternals
$prt = Get-AADIntUserPRTToken
Write-Host "PRT Cookie: $prt"

# Utilisation du PRT pour acceder a des ressources M365
$at = Get-AADIntAccessTokenForEXO -PRTToken $prt
Read-AADIntUserMail -AccessToken $at

# Protection : verifier que Credential Guard est actif
$guard = Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
Write-Host "Credential Guard: $($guard.EnableVirtualizationBasedSecurity)"

# Activer Credential Guard via GPO
# Computer Configuration > Administrative Templates > System > Device Guard
# "Turn On Virtualization Based Security" = Enabled
```

Device Code Flow Phishing : Un Vecteur MFA-Resistant

Le **Device Code Flow** est un flux OAuth 2.0 conçu pour les appareils sans navigateur (Smart TV, CLI tools, IoT). Il génère un code à usage unique que l'utilisateur entre sur un site Microsoft pour

s'authentifier. Les attaquants ont détourné ce mécanisme en 2024-2026 pour du phishing ciblé : ils génèrent un code Device Code avec leurs outils, envoient ce code à la victime via un email ou un SMS d'apparence légitime ("votre session Microsoft 365 a expiré, entrez ce code pour vous reconnecter"), et récupèrent le token d'authentification résultant.

La particularité du Device Code Flow est qu'il contourne complètement le MFA : puisque c'est l'attaquant qui génère le code et attend que la victime l'entre sur le site Microsoft, l'authentification MFA est effectuée par la victime elle-même, et le token résultant est capturé par l'attaquant. Il n'y a pas de proxy man-in-the-middle — c'est l'API OAuth standard de Microsoft qui est utilisée.

```
 # Demonstration Device Code Flow phishing (environnement de test uniquement)
Import-Module TokenTactics
Get-AzureToken -Client MSGraph

# Resultat : l'outil affiche un code et une URL
# L'attaquant envoie : "Entrez le code A1B2C3 sur https://microsoft.com/devicelogin"
# Quand la victime l'entre et s'authentifie (avec MFA inclus), l'attaquant recupere le toke

# Mitigation : Conditional Access Policy pour bloquer Device Code Flow
# New-AzureADMSConditionalAccessPolicy (via PowerShell ou portail Entra)
# Condition : Authentication Flows = Device Code Flow
# Grant Control : Block
```

OAuth Application Abuse : Le Consentement Malveillant

Les attaques via des applications OAuth malveillantes (souvent appelées "consent phishing" ou "illicit consent grant") consistent à enregistrer une application dans Entra ID avec des permissions larges, puis à convaincre un administrateur de consentir à ces permissions via un lien de phishing. Une fois le consentement accordé, l'application dispose d'un accès persistant aux ressources de l'utilisateur ou du tenant, accessible via des client credentials (sans interaction utilisateur ni MFA).

```
 # Detection des applications OAuth avec permissions larges via Graph API
GET https://graph.microsoft.com/v1.0/servicePrincipals?filter=appRoles/any(a:a/value eq 'Us

# PowerShell : lister les consentements accordes recemment
Connect-MgGraph -Scopes "Application.ReadWrite.All"
Get-MgServicePrincipal -Filter "createdDateTime ge 2026-01-01" | Select-Object DisplayName,

# Audit des permissions accordees par les utilisateurs (delegated permissions)
Get-MgOauth2PermissionGrant | Where-Object {$_.Scope -like "*ReadWrite*"} | Select-Object C

# Politique de prevention : restreindre le consentement utilisateur
# Entra ID > Enterprise Applications > User settings
# "Users can consent to apps" = Non (admin consent required)
```

Le rôle du SOC dans la Détection BadSuccessor et des Attaques Entra ID

La détection efficace de BadSuccessor et des attaques Entra ID nécessite un SOC correctement configuré avec des playbooks spécifiques. Les équipes SOC doivent disposer d'une visibilité sur quatre sources de données distinctes : les logs de sécurité Windows des DC (événements 4741, 5136, 4776), les logs Entra ID Sign-In et Audit Logs, les alertes Microsoft Defender for Identity (MDI) et les alertes Microsoft Defender for Cloud Apps.

Le playbook recommandé pour une alerte "dMSA créé avec PrecededByLink suspect" doit inclure : isolation du compte dMSA (désactivation immédiate), revue des actions effectuées avec ce compte depuis sa création (logs Kerberos et accès aux ressources), identification de l'utilisateur ayant créé le dMSA (événement 4741 avec SubjectUserName), évaluation de si ce compte a obtenu des droits Tier 0 (accès aux DC, AD CS, ADFS), et si oui, déclenchement de la procédure de compromission de domaine.

```
 # Playbook SOC BadSuccessor - verifications post-alerte
# 1. Identifier le compte createur du dMSA suspect
Get-WinEvent -ComputerName "dc01" -FilterHashtable @{
    LogName="Security"; Id=4741
    StartTime=(Get-Date).AddHours(-24)
} | Where-Object {$_.Message -like "*msDS-DelegatedManagedServiceAccount*"} | Select-Object

# 2. Desactiver immediatement le dMSA suspect
Disable-ADServiceAccount -Identity "nom-dMSA-suspect"

# 3. Rechercher les connexions effectuees avec ce compte
Get-WinEvent -ComputerName "dc01" -FilterHashtable @{
    LogName="Security"; Id=4624
    StartTime=(Get-Date).AddHours(-24)
} | Where-Object {$_.Message -like "*nom-dMSA-suspect*"}
```

Conditional Access : Identifier et Combler les Angles Morts

Les **Conditional Access Policies (CAP)** d'Entra ID sont souvent configurées avec des lacunes que les attaquants exploitent systématiquement lors de la post-exploitation d'un compte compromis. Les angles morts les plus courants en 2026 sont les comptes de service exclus du MFA pour des raisons de compatibilité, les Named Locations trop larges incluant des plages IP partenaires, les applications legacy exemptées car incompatibles avec MFA moderne, et l'absence de politiques spécifiques pour les rôles admin Entra ID.

```
 # KQL Sentinel : detecter les connexions contournant Conditional Access
SigninLogs
| where ResultType == 0
| where ConditionalAccessStatus == "notApplied"
| where AppDisplayName !in ("Windows Sign In", "Microsoft Authentication Broker", "Microsof
| project TimeGenerated, UserDisplayName, AppDisplayName, IPAddress, Location, UserAgent
| sort by TimeGenerated desc

# Identifier les utilisateurs sans politiques CA applicables
SigninLogs
| where ConditionalAccessStatus == "notApplied"
| summarize count() by UserPrincipalName
| sort by count_ desc
```

Pass-the-Certificate vers Entra ID : Technique Hybride Avancée

Dans les environnements hybrides avec AD CS, la technique **Pass-the-Certificate** permet d'utiliser un certificat AD CS valide pour s'authentifier auprès d'Entra ID via PKINIT (Windows Hello for Business ou certificat client), puis d'obtenir un PRT. Cette technique combine une compromission AD CS on-premises avec une persistance dans Entra ID cloud — créant un vecteur de compromission cross-cloud particulièrement difficile à détecter et à remédier car il implique deux systèmes distincts avec des équipes et des outils de monitoring souvent différents.

```
 # Pass-the-Certificate vers Entra ID via Certipy et ROADtools
# Etape 1 : Obtenir un certificat pour le compte cible via ADCS compromis
certipy req -u utilisateur@domaine.local -p motdepasse -ca CA-Name -template User -dc-ip dc

# Etape 2 : Utiliser le certificat pour l'auth Entra ID
python3 roadtx.py gettokens --prt-method certlogin --pfx-file utilisateur.pfx --pfx-pass mo

# Etape 3 : Acceder aux ressources M365 avec le PRT obtenu
python3 roadtx.py browsewithprt --prt-file user.prt --url https://outlook.office.com
```

Continuous Access Evaluation (CAE) : Protection et Limites

Le **Continuous Access Evaluation (CAE)** est une fonctionnalité Entra ID qui permet aux applications compatibles de recevoir des signaux de révocation de token en temps quasi-réel (moins d'une minute) au lieu d'attendre l'expiration normale du token (60 minutes). Si un utilisateur est désactivé, si son mot de passe est modifié, ou si sa session est révoquée, les applications CAE-compatibles reçoivent immédiatement un signal pour forcer une nouvelle authentification.

Cependant, CAE ne protège que pour les applications qui l'implémentent explicitement. Microsoft Exchange Online, SharePoint Online et Teams le supportent, mais de nombreuses applications tierces ne le font pas encore. Pour les applications non-CAE, un token volé reste valide pendant toute sa durée de vie (60 minutes à 1 heure par défaut, ou jusqu'à 1 an pour les tokens de refresh).

Hardening Entra ID : Configuration de Sécurité Prioritaire 2026

La protection d'Entra ID contre les attaques modernes passe par une configuration rigoureuse suivant le principe du moindre privilège et de la défense en profondeur :

Bloquer Device Code Flow via une Conditional Access Policy pour tous les utilisateurs standard

Restreindre le consentement OAuth — exiger le consentement administrateur pour toutes les applications tiers

Activer Token Protection (preview) pour lier les tokens au device physique

PIM pour tous les rôles admin avec activation JIT et approbation par un pair

Authentication Strengths — exiger FIDO2 pour les rôles Global Admin et Privileged Role Admin

Activer CAE et surveiller les applications qui ne le supportent pas

Contrôle Entra ID	Vecteur bloqué	Effort	Statut
FIDO2 pour admins	Device Code phishing, PRT theft	Moyen	GA 2026
Token Protection	Token replay depuis autre machine	Faible	Preview
CAP Device Code Block	Device Code Flow phishing	Faible	GA
CAE activé	Session persistence post-compromission	Moyen	GA
Admin Consent Required	OAuth consent phishing	Faible	GA

Entra ID Identity Protection et Hybrid Identity Security Score

Microsoft Entra ID Protection utilise le machine learning pour détecter les comportements d'authentification anormaux et générer des alertes de risque. Les signaux analysés incluent la réputation IP, la vitesse de déplacement impossible (connexion depuis deux pays en moins d'une heure), les attributs de device inconnu, et les patterns comportementaux atypiques. Pour BadSuccessor et les attaques Entra ID, Identity Protection peut détecter certains indicateurs comportementaux post-compromission, mais la détection précoce nécessite la combinaison Identity Protection + MDCA + règles SIEM personnalisées.

Le **Microsoft Secure Score** mesure la posture de sécurité globale du tenant avec des recommandations spécifiques Entra ID incluant : activer Identity Protection (+5%), imposer MFA à tous les utilisateurs (+10%), bloquer l'authentification legacy (+7%), activer PIM pour les rôles privilégiés (+8%). Ces recommandations sont directement liées à la réduction de l'exposition aux attaques Entra ID documentées dans cet article.

```
 # KQL Sentinel : alertes Identity Protection haut risque
AADRiskyUsers
| where RiskLevel == "high"
| where RiskState == "atRisk"
| project TimeGenerated, UserDisplayName, RiskLevel, RiskDetail
| sort by TimeGenerated desc

# Correlater avec les connexions recentes des utilisateurs a risque
let risky = AADRiskyUsers | where RiskLevel in ("high","medium") | distinct UserPrincipalNa
SigninLogs
| where UserPrincipalName in (risky)
| where ResultType == 0
| project TimeGenerated, UserPrincipalName, IPAddress, AppDisplayName, Location
```

Attaques OIDC et Abus des Applications OAuth dans Entra ID

Au-delà de SAML/ADFS, les applications **OAuth 2.0/OIDC** représentent une surface d'attaque croissante. Les techniques incluent le vol de refresh tokens OAuth (durée de vie longue, pas de MFA au renouvellement), l'abus des scopes excessifs accordés à des applications tier, et l'exploitation des implicit grant flows. La correction passe par l'audit des scopes OAuth accordés, la désactivation du flow implicit et l'activation de PKCE (Proof Key for Code Exchange) pour les nouvelles applications.

```
 # Audit des consentements OAuth accordes avec scopes larges
Connect-MgGraph -Scopes "Application.ReadWrite.All"
Get-MgOauth2PermissionGrant | Where-Object {$_.Scope -like "*ReadWrite*"} | Select-Object C

# Identifier les applications utilisant le flow implicite (a migrer vers code flow + PKCE)
Get-MgApplication | Where-Object {$_.Spa.RedirectUris.Count -gt 0} | Select-Object DisplayN

# Politique de prevention : exiger le consentement admin pour toutes les apps tiers
# Entra ID > Enterprise Applications > User settings > "Users can consent to apps" = Non
```

Service Principals : Le Point Aveugle de la Gouvernance Entra ID

Les **service principals** Entra ID (équivalents cloud des comptes de service AD) représentent un angle mort majeur dans la gouvernance des identités cloud. De nombreuses organisations ont des centaines ou milliers de service principals créés au fil des années, avec des permissions largement supérieures au nécessaire et sans rotation régulière des secrets (client secrets ou certificats). La compromission d'un secret de service principal avec des permissions larges (User.ReadWrite.All, Mail.ReadWrite, etc.) permet un accès persistant aux ressources Microsoft 365 sans interaction interactive ni MFA.

```
 # Audit des service principals avec permissions larges
Connect-MgGraph -Scopes "Application.ReadWrite.All,AppRoleAssignment.ReadWrite.All"
Get-MgServicePrincipal -All | ForEach-Object {
    $appRoles = Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $_.Id
    $appRoles | Where-Object {$_.ResourceDisplayName -eq "Microsoft Graph"} | ForEach-Objec
        [PSCustomObject]@{
            App=$_.PrincipalDisplayName
            Permission=Get-MgServicePrincipalAppRole -ServicePrincipalId $_.ResourceId | Wh
        }
    }
}

# Identifier les client secrets expires depuis plus de 6 mois (risque de rotation manquee)
Get-MgApplication | ForEach-Object {
    $_.PasswordCredentials | Where-Object {$_.EndDateTime -lt (Get-Date)} | ForEach-Object
        Write-Warning "Secret expire pour app : $(Get-MgApplication -ApplicationId $_.KeyId
    }
}
```

Ressources Microsoft et MITRE sur BadSuccessor et Entra ID

Documentation officielle

MITRE ATT&CK T1606 : Forge Web Credentials (SAML et tokens)

Microsoft Security Blog : BadSuccessor et mesures d'atténuation

Intégration dans les Tests de Pénétration : BadSuccessor et Entra ID

Pour les équipes red team, BadSuccessor est désormais un test systématique à inclure dans toute évaluation d'environnement Windows Server 2025. Les conditions d'exploitation sont vérifiables rapidement avec un audit des délégations CreateChild et la présence de WS2025. Côté Entra ID, les tests de Device Code Flow phishing et d'abus de service principals font partie du standard des pentests cloud en 2026.

Pour les aspects de détection SOC, notre article sur la détection d'attaques Azure AD fournit les règles SIEM nécessaires. Pour les vecteurs BadSuccessor dans le contexte AD on-premises, consultez notre analyse des 10 attaques AD les plus critiques. Pour la gouvernance des identités cloud, notre guide Zero Trust Microsoft 365 fournit le cadre architecturale adapté.

Entra Connect SyncJacking : Compromission Bidirectionnelle

Une technique documentée en 2025, le **SyncJacking d'Entra Connect**, exploite le composant de synchronisation entre l'AD on-premises et Entra ID. En compromettant le serveur Entra

Connect (anciennement Azure AD Connect), un attaquant peut modifier les attributs synchronisés vers le cloud, créer des comptes cloud fantômes avec des droits élevés, ou bloquer la synchronisation pour empêcher la révocation de comptes compromis.

Notre article dédié sur Entra Connect SyncJacking et mesures de blocage détaille cette technique spécifique et les contre-mesures. Le point clé est que le serveur Entra Connect doit être traité comme un asset Tier 0 car sa compromission permet un impact cloud équivalent à une compromission de Domain Controller.

Correlation BadSuccessor et Attaques Entra : La Chaîne Cross-Cloud

La combinaison la plus dangereuse en 2026 est la chaîne BadSuccessor on-premises + exploitation Entra ID cloud. L'attaquant utilise BadSuccessor pour obtenir des droits Domain Admin en quelques minutes depuis un compte helpdesk, puis exploite les permissions Entra Connect pour synchroniser un compte malveillant vers le tenant Entra ID avec des droits Global Admin. Une fois dans Entra ID, il crée des backdoors (application OAuth avec permissions larges, service principal avec client secret à longue durée de vie) qui persistent même après la remédiation on-premises.

Cette chaîne cross-cloud est particulièrement difficile à détecter car elle implique deux environnements avec des équipes et des outils distincts : l'équipe infrastructure Windows pour l'AD on-premises, et l'équipe cloud pour Entra ID. La coordination entre ces équipes lors d'une réponse à incident est un facteur critique souvent sous-estimé.

BadSuccessor vs dCShadow : Comparaison des Vecteurs dMSA

BadSuccessor est parfois comparé à dCShadow (introduit par Benjamin Delpy en 2018), qui permettait d'injecter des objets AD arbitraires en se faisant passer pour un contrôleur de domaine temporaire. Les deux techniques partagent l'idée d'abuser de mécanismes légitimes AD pour

effectuer des modifications non autorisées. Cependant, BadSuccessor est significativement plus simple à exploiter car il ne nécessite pas d'élever ses privilèges à Domain Admin (prérequis de dCShadow) — un simple droit CreateChild suffit. C'est pourquoi l'impact potentiel de BadSuccessor est considéré plus élevé que dCShadow dans les évaluations de risque 2026.

Audit Active Directory Post-BadSuccessor : Liste de Vérification

Pour les organisations ayant déployé Windows Server 2025 (ou planifiant de le faire), voici la liste de vérification post-BadSuccessor à exécuter immédiatement :

Lister tous les dMSA existants et vérifier leur attribut PrecededByLink — tout dMSA pointant vers un compte privilégié est suspect

Auditer toutes les délégations CreateChild sur les OUs, en particulier pour les comptes helpdesk, les équipes IT de niveau 1 et les comptes de service

Activer l'audit des modifications d'objets AD (5136) pour les classes msDS-DelegatedManagedServiceAccount

Restreindre la création de dMSA aux seuls administrateurs Tier 0 — si les dMSA ne sont pas utilisés, supprimer complètement le droit de création

Mettre à jour vers la dernière version de Windows Server 2025 qui inclut les mesures d'atténuation Microsoft

```powershell
 # Checklist rapide BadSuccessor (PowerShell)
Write-Host "=== Verification BadSuccessor ===" -ForegroundColor Yellow

# 1. Machines WS2025 dans le domaine
$ws2025 = Get-ADComputer -Filter * -Properties OperatingSystem | Where-Object {$_.Operating
Write-Host "Machines WS2025: $($ws2025.Count)"

# 2. dMSA existants
$dmsas = Get-ADObject -Filter {objectClass -eq "msDS-DelegatedManagedServiceAccount"} -Prop
Write-Host "dMSA trouves: $($dmsas.Count)"
if ($dmsas.Count -gt 0) { $dmsas | Format-Table Name,"msDS-ManagedAccountPrecededByLink" }

# 3. OUs avec delegation CreateChild non-heritee
$ous = Get-ADOrganizationalUnit -Filter *
foreach ($ou in $ous) {
    $acl = Get-Acl -Path "AD:\$($ou.DistinguishedName)"
    $createChild = $acl.Access | Where-Object {$_.ActiveDirectoryRights -like "*CreateChild
    if ($createChild) { Write-Warning "OU avec CreateChild delegue: $($ou.Name)" }
}
```

Impact sur les Organisations Françaises : Contexte NIS 2 et ANSSI

Les vulnérabilités comme BadSuccessor illustrent pourquoi l'ANSSI insiste sur la nécessité d'un programme de gestion des vulnérabilités incluant le suivi actif des nouvelles techniques d'attaque AD, au-delà du simple déploiement des patches CVE classiques. BadSuccessor n'est pas un CVE traditionnel — c'est l'abus d'un comportement de conception — ce qui le rend invisible aux scanners de vulnérabilités traditionnels comme Nessus ou Qualys.

Pour les entités soumises à NIS 2, une revue de la posture AD contre BadSuccessor est maintenant attendue dans le cadre des mesures de sécurité Article 21. L'ANSSI a mis à jour ses recommandations AD pour inclure spécifiquement les précautions relatives aux dMSA et Windows Server 2025.

Foire Aux Questions sur BadSuccessor et les Attaques Entra ID

BadSuccessor affecte-t-il tous les environnements Active Directory ?

Non. BadSuccessor nécessite la présence de Windows Server 2025 dans le domaine. Les environnements exclusivement Windows Server 2019/2022 ne sont pas directement vulnérables à l'exploitation via dMSA. Cependant, tout environnement qui planifie un upgrade vers WS2025 doit auditer ses délégations CreateChild et restreindre la création de dMSA avant ou immédiatement après le déploiement. La vérification rapide se fait en listant les OUs avec délégations CreateChild non héritées : si ce nombre est supérieur à 5-10, une revue complète s'impose avant tout upgrade WS2025.

Le MFA Entra ID protège-t-il contre le PRT theft ?

Partiellement. Si un attaquant parvient à extraire un PRT valide de la mémoire d'une machine (nécessite un accès admin local), il peut l'utiliser pour obtenir des access tokens sans déclencher une nouvelle demande MFA, car le PRT certifie que le MFA a déjà été effectué lors de l'authentification initiale de l'utilisateur légitime. La protection efficace contre le PRT theft est l'activation de Credential Guard avec TPM 2.0 qui lie le PRT au hardware — rendant son extraction purement logicielle impossible. Token Protection en preview dans Entra ID offre une couche supplémentaire en liant cryptographiquement le token à l'empreinte du device.

Comment détecter rapidement si des dMSA BadSuccessor ont été créés dans mon domaine ?

La détection est rapide via PowerShell : Get-ADObject -Filter {objectClass -eq "msDS-DelegatedManagedServiceAccount"} -Properties "msDS-ManagedAccountPrecededByLink","Created" retourne tous les dMSA existants avec leur compte précédent. Tout dMSA dont le PrecededByLink pointe vers un compte appartenant aux groupes Domain Admins, Enterprise Admins ou Protected Users est suspect et doit être immédiatement supprimé et investigué. Dans un environnement sain sans utilisation volontaire de dMSA, le résultat de cette requête devrait être vide.

Gouvernance du Cycle de Vie des Identités Entra ID : Prévenir les Attaques à la Source

La plupart des attaques Entra ID documentées en 2026 exploitent des failles dans la gouvernance du cycle de vie des identités : comptes non désactivés après départ d'employé, service principals créés lors d'un projet pilote et jamais supprimés, secrets d'application dont la date d'expiration a été fixée à "jamais expirer" il y a trois ans. La gouvernance du cycle de vie est la première ligne de défense, avant même les Conditional Access Policies ou Defender for Identity.

En pratique, les organisations françaises que nous auditons présentent régulièrement les mêmes patterns de risque : des service principals créés par des équipes de développement avec des permissions **Directory.ReadWrite.All** "le temps d'un sprint", des comptes invités B2B non revus depuis 18 mois, et des applications d'entreprise autorisées par des utilisateurs sans revue de leurs permissions déléguées. Ces trois catégories constituent les vecteurs d'entrée favoris des attaquants ciblant Entra ID en 2026, car ils offrent des chemins d'accès privilégiés sans nécessiter de vol de credentials.

Vecteur de risque	Fréquence observée	Impact potentiel	Remédiation prioritaire
Service principals avec permissions larges	Très élevée (85% des tenants)	Accès à toutes les données tenant	Audit permissions, rotation secrets 90j
Comptes invités B2B non revus	Élevée (72% des organisations)	Accès persistant non supervisé	Access Reviews trimestrielles obligatoires
Device Code Flow non restreint	Très élevée (91% des tenants)	Phishing MFA bypass	Bloquer via Conditional Access Policy
Comptes admin sans PIM	Élevée (68% PME)	Compromission admin permanente	Activation PIM obligatoire pour tous les rôles
Legacy authentication activée	Moyenne (45% organisations)	Bypass MFA via IMAP/ POP3/SMTP	Bloquer protocols hérités via CA Policy

Les *Entra ID Access Reviews* sont l'outil central de la gouvernance du cycle de vie. Configurées sur une base trimestrielle au minimum, elles forcent les propriétaires d'applications et les managers à revalider les accès de leurs équipes. Sans cette validation active, les accès s'accumulent par inertie organisationnelle et créent une surface d'attaque croissante. L'ANSSI, dans son guide "Sécurité des systèmes d'information cloud" de 2025, recommande explicitement la mise en place d'Access Reviews comme mesure de gouvernance minimale pour les organisations adoptant Microsoft 365.

Entitlement Management et Packages d'Accès : Réduire l'Exposition BadSuccessor

Pour réduire le risque BadSuccessor à sa source — les délégations CreateChild sur les OUs — l'approche recommandée est l'**Entitlement Management** d'Entra ID, qui permet de créer des "packages d'accès" regroupant permissions AD et cloud avec un processus d'approbation et une durée de vie limitée. Plutôt que de déléguer CreateChild de manière permanente à l'équipe helpdesk, on crée un package d'accès "Création comptes OU Marketing" valable 6 mois, nécessitant l'approbation du responsable RH, et révocable immédiatement.

Cette approche réduit la surface d'exposition BadSuccessor en limitant le nombre de comptes détenant le droit CreateChild à un instant donné, en traçant chaque attribution dans les logs Entra ID, et en imposant une revue régulière. C'est l'application du principe du **moindre privilège juste-à-temps** au niveau des délégations AD, un concept que l'on retrouve dans le modèle Tier d'Active Directory mais appliqué au niveau des droits d'objet individuels.

```
 # Audit des service principals a risque dans Entra ID (Microsoft Graph PowerShell)
Connect-MgGraph -Scopes "Application.Read.All","Directory.Read.All"

# Lister les service principals avec des permissions sensibles
$dangerousPermissions = @(
    "Directory.ReadWrite.All",
    "RoleManagement.ReadWrite.Directory",
    "AppRoleAssignment.ReadWrite.All",
    "DelegatedPermissionGrant.ReadWrite.All"
)

Get-MgServicePrincipal -All | ForEach-Object {
    $sp = $_
    $appRoles = Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $sp.Id
    $appRoles | Where-Object {$_.PrincipalType -eq "ServicePrincipal"} | ForEach-Object {
        $roleDef = Get-MgServicePrincipalAppRole -ServicePrincipalId $_.ResourceId | Where-
        if ($dangerousPermissions -contains $roleDef.Value) {
            Write-Warning "SP risque: $($sp.DisplayName) | Permission: $($roleDef.Value)"
        }
    }
}

# Verifier les secrets sans date d'expiration
Get-MgApplication -All | ForEach-Object {
    $app = $_
    $_.PasswordCredentials | Where-Object {$_.EndDateTime -gt (Get-Date).AddYears(2)} | For
        Write-Warning "Secret long terme (>2ans): App=$($app.DisplayName), Expire=$($_.EndD
    }
}
```

Hardening Avancé : Workload Identity Federation et Élimination des Secrets

L'approche la plus radicale pour neutraliser les attaques basées sur le vol de secrets de service principals est l'élimination des secrets eux-mêmes via la **Workload Identity Federation**. Cette technologie permet aux applications s'exécutant sur des plateformes comme Azure Kubernetes Service, GitHub Actions, ou des VMs avec identité managée d'obtenir des tokens Entra ID sans jamais avoir besoin d'un client secret ou d'un certificat.

Le principe : la plateforme d'exécution (ex. GitHub Actions) génère un token OIDC signé par GitHub. L'application présente ce token à Entra ID, qui vérifie la signature et émet un token Entra ID en retour. Aucun secret à stocker, à faire tourner, ou à voler. Pour les nouvelles applications, la Workload Identity Federation devrait être le standard par défaut, réservant les client secrets aux seuls cas d'usage n'ayant pas accès à une plateforme compatible OIDC.

Réponse à Incident : Playbook Combiné BadSuccessor et Entra ID

Lors d'une suspicion de compromission BadSuccessor ou d'attaque Entra ID, le temps de réaction est critique. Voici les actions immédiates à exécuter dans les premières 60 minutes, structurées par équipe :

Équipe Infrastructure AD (0-30 min) : Lister tous les dMSA créés dans les dernières 24-72 heures (`Get-ADObject -Filter {objectClass -eq "msDS-DelegatedManagedServiceAccount"} -Properties Created | Where-Object {$_.Created -gt (Get-Date).AddDays(-3)}`), suspendre immédiatement tout dMSA suspect, identifier le compte ayant créé l'objet malveillant via les logs 5137, réinitialiser le mot de passe du compte compromis, et activer le tier 0 lockdown si la compromission est confirmée.

Équipe Cloud Entra ID (0-30 min) : Dans le portail Microsoft Entra, revocation des sessions (*Révoquer toutes les sessions* pour le compte suspect), désactivation du compte utilisateur concerné, revue des connexions récentes dans les logs de connexion (filtrage sur le pays d'origine, l'IP, le user agent), et vérification des applications auxquelles le compte a accordé des consentements récemment.

Équipe SOC (30-60 min) : Corrélation des événements AD (5137 creation dMSA) avec les logs Entra ID (token issuance, application consent), identification des comptes ayant interagi avec le compte compromis dans les 48h précédentes, vérification de l'absence de nouveaux service principals créés avec des permissions larges, et activation des alertes Defender XDR pour surveillance renforcée pendant 72h.

Benchmark de Maturité Sécurité Identité : Où se Situe Votre Organisation ?

Pour évaluer objectivement la posture de sécurité identité d'une organisation face aux risques BadSuccessor et Entra ID 2026, il est utile de se positionner sur une échelle de maturité à quatre niveaux. Ce benchmark est utilisé par les équipes RSSI pour prioriser les investissements et argumenter les demandes budgétaires auprès de la direction générale.

Niveau 1 — Exposé : Aucun audit des délégations AD, Device Code Flow non restreint, MFA non imposé sur tous les comptes admin, aucune Access Review sur les service principals. Ce niveau décrit malheureusement encore une fraction significative des PME et ETI françaises que nous rencontrons lors de missions de conseil. Ces organisations représentent des cibles de choix pour les groupes APT et ransomware car leur surface d'attaque identité est maximale et leur capacité de détection minimale.

Niveau 2 — Basique : MFA déployé sur tous les comptes utilisateurs et admins, Conditional Access Policies actives pour les connexions à risque élevé, mais sans restriction du Device Code Flow ni audit régulier des service principals. Les délégations AD sont documentées mais jamais révisées. À ce niveau, l'organisation résiste aux attaques opportunistes mais reste vulnérable aux attaquants ciblés qui exploitent BadSuccessor ou les vecteurs Entra ID documentés.

Niveau 3 — Avancé : Toutes les mesures de niveau 2, plus : PIM activé pour tous les rôles Entra ID et AD, Device Code Flow bloqué, CAE activé sur les applications critiques, Access Reviews trimestrielles sur les comptes invités et service principals, Credential Guard avec TPM 2.0 sur tous les postes admins. À ce niveau, l'organisation détecte la majorité des techniques BadSuccessor et Entra ID si elle a configuré Defender for Identity et Sentinel avec les règles de détection appropriées.

Niveau 4 — Expert : Niveau 3 plus Workload Identity Federation (zéro client secret), Token Protection activé, exercices red team cross-cloud annuels, CIEM (Cloud Infrastructure Entitlement Management) déployé pour audit continu des permissions, intégration complète AD et Entra ID dans le SIEM avec corrélation cross-domaine. Ce niveau correspond aux grandes organisations avec des équipes sécurité dédiées et des budgets adaptés — mais ses principes directeurs (moindre privilège, rotation automatique, monitoring continu) restent applicables à toute échelle.

Opinion : La Frontière AD/Cloud est Morte, Pensez Identité Unifiée

La séparation traditionnelle entre la sécurité AD on-premises et la sécurité cloud Entra ID est devenue une fiction organisationnelle dangereuse. BadSuccessor illustre comment une vulnérabilité dans un nouveau mécanisme AD (dMSA Windows Server 2025) peut, en quelques étapes, aboutir à une compromission complète d'un tenant Microsoft 365. Maintenir deux équipes distinctes avec des outils distincts et des processus distincts pour gérer ces deux environnements crée des angles morts systématiques que les attaquants exploitent méthodiquement.

La réponse n'est pas de fusionner les équipes (ce qui pose des problèmes organisationnels réels) mais d'imposer des *exercices red team cross-cloud* annuels où les scénarios testent explicitement les chaînes d'exploitation qui traversent la frontière on-premises/cloud. Une organisation qui n'a jamais testé la chaîne "helpdesk compromise → BadSuccessor → Entra Connect → tenant takeover" ne peut pas affirmer avec confiance qu'elle serait capable de détecter et d'endiguer cette attaque dans un contexte réel. C'est cette honnêteté face à ses propres lacunes qui distingue les organisations cyber-matures des organisations qui se croient protégées.

Les certifications comme ISO 27001 et la mise en conformité NIS 2 imposent une vision holistique de la sécurité des systèmes d'information — et les annex controls de l'ISO 27001:2022 (notamment A.5.15 sur le contrôle d'accès et A.5.16 sur la gestion des identités) s'appliquent sans distinction entre on-premises et cloud. Les auditeurs de certification commencent à poser des questions spécifiques sur la segmentation des comptes d'administration entre les deux

environnements et sur les procédures de révocation d'urgence cross-domaine. Se préparer à ces questions est une opportunité pour élever le niveau de maturité global de la sécurité identité.

À RETENIR

Points clés BadSuccessor et Entra ID Attacks 2026

BadSuccessor nécessite uniquement CreateChild sur une OU pour compromettre n'importe quel compte du domaine — un droit souvent délégué au helpdesk

Auditer immédiatement les délégations CreateChild est urgent pour tout domaine utilisant Windows Server 2025

Le PRT theft contourne le MFA — Credential Guard avec TPM 2.0 est la défense matérielle indispensable

Device Code Flow doit être bloqué via Conditional Access pour tous les utilisateurs standard

Les service principals sont le talon d'Achille d'Entra ID — rotation des secrets et audit des permissions sont non négociables

Token Protection (preview) est la prochaine évolution clé pour protéger les tokens contre le replay inter-machines

CAE activé sur les applications critiques réduit la fenêtre d'exploitation d'un token volé de 60 minutes à moins d'une minute

© Ayi NEDJIMI Consultants — Tous droits réservés