AYI NEDJIMI Consultants

LOLBas / LOLBins : Living Off The La

30 April 2026 • Mis à jour le 30 April 2026 • 49 min de lecture

Guide complet LOLBas/LOLBins : certutil, mshta, rundll32, regsvr32, BYOV défense AppLocker/WDAC.

Les techniques de **Living Off the Land (LOL)** représentent l'une des évolutions les cybernétiques contemporaines, permettant aux attaquants d'exploiter les outils et d'exploitation Windows pour exécuter des actions malveillantes sans déployer de the Land Binaries, Scripts and Libraries) documente systématiquement ces binaire peuvent être détournés à des fins offensives — de l'exécution de code arbitraire a l'évasion des défenses, la persistance et l'exfiltration de données. Des outils comm **wmic**, **bitsadmin** et **cmstp** sont présents sur chaque installation Windows et signé implicite auprès des solutions de sécurité traditionnelles. Les groupes APT les plus **Group**, en passant par **APT41** et **FIN7** — intègrent massivement ces techniques da solutions EDR et les politiques d'exécution restrictives. Ce guide expert analyse en techniques d'exploitation avancées, les campagnes APT documentées, et les stra **Sysmon**, les **règles Sigma**, **AppLocker** et **WDAC** pour neutraliser ces menaces qu du système d'exploitation lui-même.

À RETENIR

Points clés de cet article :

- Les LOLBins sont des binaires Windows légitimes signés par Microsoft qui le téléchargement et l'évasion
- Le projet LOLBAS (lolbas-project.github.io) catalogue plus de 200 binaires Windows
- certutil, mshta, rundll32, regsvr32 et bitsadmin sont les LOLBins les plus
- Les LOLDrivers (Bring Your Own Vulnerable Driver - BYOVD) permettent le désactiver les solutions de sécurité au niveau kernel
- La détection repose sur Sysmon (événements 1, 3, 7, 11), les règles Sigma
- AppLocker et WDAC (Windows Defender Application Control) constituent les LOLBins
- Le script block logging PowerShell et la transcription sont essentiels pour

Fondamentaux du Living Off the Land

Le concept de Living Off the Land (littéralement "vivre de la terre") en cybersécur binaires et fonctionnalités déjà présents sur le système cible, plutôt que le déploie plusieurs avantages tactiques majeurs : les binaires utilisés sont signés par Micros permet de contourner les politiques d'exécution basées sur les signatures numéri installation Windows standard, garantissant la fiabilité des techniques indépendam cible ; leur utilisation légitime par les administrateurs système crée un bruit de fon usage normal et malveillant ; et ils ne nécessitent pas de télécharger ou déposer d permettant des attaques partiellement ou totalement "fileless".