Exploitation Kernel Windows 2026 : Drivers et Bypass KASLR

> Exploitation kernel Windows 2026 — BYOVD, drivers vulnérables, KASLR bypass, PPL bypass et contre-mesures HVCI pour organisations françaises soumises à NIS 2.

En janvier 2025, un groupe APT a compromis plusieurs organisations françaises du secteur de la défense en exploitant une technique BYOVD (Bring Your Own Vulnerable Driver) combinant un driver légitime mais vulnérable d'un logiciel de monitoring populaire avec une exploitation du noyau Windows permettant de désactiver les solutions EDR installées sur les systèmes cibles. Cette technique, documentée par le CERT-FR dans un bulletin de sécurité urgent, illustre l'évolution des tactiques d'exploitation du noyau Windows que les équipes de sécurité françaises doivent comprendre et savoir contrer en 2026. L'exploitation du noyau Windows représente la menace la plus grave en termes d'impact potentiel, car un attaquant disposant de l'exécution de code en mode noyau (Ring 0) a un contrôle total et pratiquement invisible sur le système, capable de désactiver n'importe quelle protection logicielle, de manipuler les processus système, d'accéder directement à la mémoire physique, et de persister à travers les redémarrages et même les réinstallations du système d'exploitation dans certains cas de compromission très avancée impliquant une persistance au niveau du firmware. Ce guide technique complet présente les techniques d'exploitation du noyau Windows en 2026 — **BYOVD**, bypass KASLR, contournement PPL, et exploitation de drivers vulnérables — ainsi que les contre-mesures défensives déployées par Microsoft (HVCI, Kernel Data Protection, Vulnerable Driver Blocklist via WDAC) et les recommandations pratiques pour les équipes de sécurité françaises qui doivent évaluer et renforcer leur posture de protection contre ces menaces avancées. Ce guide s'adresse aux analystes SOC, aux équipes Red Team, aux pentesters et aux RSSI techniques qui souhaitent comprendre en profondeur les mécanismes d'attaque et de défense au niveau du noyau Windows dans les environnements de production actuels soumis aux exigences ANSSI et NIS 2. La complexité technique de ces attaques ne doit pas décourager les équipes défensives : les contre-mesures disponibles nativement dans Windows 11 et déployables via Intune sont suffisamment

efficaces pour bloquer la grande majorité des techniques documentées à condition d'être correctement configurées et maintenues à jour.

À RETENIR

À retenir

• **BYOVD** (Bring Your Own Vulnerable Driver) est la technique dominante d'exploitation kernel en 2026 — LOLDrivers.io recense 800+ drivers vulnérables

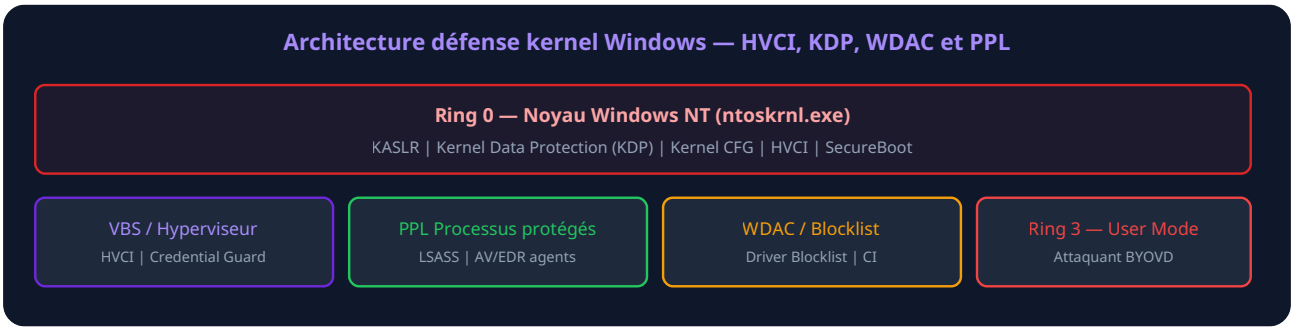
• **HVCI** (Hypervisor-Protected Code Integrity) bloque l'injection de code non signé dans le noyau — activation obligatoire sur les systèmes sensibles

• La **Vulnerable Driver Blocklist** Microsoft est mise à jour mensuellement et doit être déployée via WDAC sur tous les endpoints Windows

• **KASLR** (Kernel ASLR) est contournable via les primitives de lecture mémoire des drivers BYOVD — ne pas en faire la seule défense

• **Kernel Data Protection (KDP)** protège les structures de données noyau contre la modification — disponible sur Windows 10 20H1 avec HVCI

• Le CERT-FR recommande d'activer HVCI sur tous les systèmes Windows 11 des organisations OIV et OSE soumises aux exigences NIS 2



Architecture du noyau Windows : Ring 0 vs Ring 3 et surfaces d'attaque

Le noyau Windows s'exécute en **Ring 0** (mode noyau), le niveau le plus privilégié de l'anneau de protection x86-64, avec un accès direct à tous les registres hardware, à la mémoire physique complète, et à toutes les instructions machine sans restriction. Les applications utilisateur s'exécutent en **Ring 3** (mode utilisateur), avec un accès limité à la mémoire virtuelle allouée par le noyau. L'escalade de privilèges du Ring 3 vers le Ring 0 est l'objectif final de toute exploitation kernel, car un attaquant disposant de l'exécution de code en mode noyau a un contrôle total et pratiquement invisible sur le système : il peut désactiver toute protection logicielle, manipuler les processus système, accéder directement à la mémoire physique, et persister à travers les redémarrages sans que les outils de sécurité user-mode puissent le détecter ou le stopper sans l'aide de mécanismes hardware comme HVCI.

La surface d'attaque du noyau Windows comprend plusieurs vecteurs exploités dans des incidents réels documentés par le CERT-FR en 2024 et 2025 : les **drivers kernel** (fichiers .sys chargés en espace noyau avec tous les privilèges Ring 0), les **syscalls** (interface entre user mode et kernel mode via la table SSDT), les **objets noyau** (processus, threads, handles) accessibles via des APIs, et les **IRP (I/O Request Packets)** pour la communication inter-drivers. La compréhension de cette architecture est essentielle pour les équipes défensives qui doivent

évaluer l'impact potentiel d'une exploitation kernel et prioriser les contre-mesures à déployer en urgence sur les systèmes les plus exposés de l'organisation selon leur criticité et leur exposition au réseau.

BYOVD : Bring Your Own Vulnerable Driver — mécanisme et vecteur dominant

La technique **BYOVD (Bring Your Own Vulnerable Driver)** consiste à charger un driver kernel Windows légitime signé qui contient une vulnérabilité permettant une lecture ou écriture arbitraire en mémoire noyau, puis exploiter cette vulnérabilité pour exécuter du code Ring 0. L'avantage de BYOVD est la disponibilité : des centaines de drivers vulnérables dans des logiciels légitimes populaires sont signés par des éditeurs reconnus et contiennent des primitives d'exploitation documentées publiquement sur la base de données LOLDrivers.io qui en recense plus de 800 en 2026.

> ⚡ **Retour terrain**
>
> Sur un test d'intrusion externe pour un groupe de BTP, j'ai exploité une CVE de 2023 sur une instance Confluence exposée sur Internet — non patchée depuis 14 mois. L'application était 'connue de l'équipe IT' comme devant être mise à jour mais la priorité n'avait jamais été accordée. En 20 minutes d'exploitation, j'avais un shell sur le serveur et accès au réseau interne. La fenêtre d'exploitation de 14 mois sur une CVE exploitée in-the-wild est malheureusement représentative.

Des exemples emblématiques utilisés dans des attaques réelles contre des organisations françaises : **gdrv.sys** (Gigabyte App Center, CVE-2018-19320) utilisé par BlackByte et Scattered Spider pour désactiver les EDR, **mhyprot2.sys** (anti-cheat Genshin Impact) utilisé par des

groupes ransomware pour tuer les processus de protection, et **dbutil_2_3.sys** (Dell, CVE-2021-21551) permettant une lecture/écriture de la mémoire physique complète. La technique BYOVD est systématiquement utilisée dans les attaques APT avancées car elle exploite la confiance accordée aux drivers signés par des éditeurs légitimes, contournant les défenses basées sur la réputation des fichiers et rendant les solutions EDR basiques incapables de détecter le chargement initial du driver malveillant avant que ses actions destructrices ne commencent. Cette technique a été utilisée dans chaque grande campagne ransomware ciblant des organisations françaises depuis 2022, selon les analyses publiées par l'ANSSI dans ses rapports sur la menace cyber.

LOLDrivers et inventaire des drivers vulnérables dans votre parc

La base de données **LOLDrivers (loldrivers.io)** est la référence communautaire des drivers Windows légitimes et signés qui contiennent des vulnérabilités exploitables en BYOVD. Elle recense pour chaque driver : le hash SHA256, la version vulnérable, la CVE associée si disponible, les primitives d'exploitation (lecture mémoire, écriture mémoire, kill processus Ring 0), et les groupes d'attaquants documentés qui l'ont utilisé. Cette base est mise à jour régulièrement par la communauté sécurité mondiale et constitue la principale source d'information pour construire des règles de détection BYOVD pertinentes.

L'inventaire des drivers vulnérables présents dans votre parc est la première étape d'une évaluation BYOVD. Le script PowerShell suivant compare les drivers installés sur un système avec les hashs de la base LOLDrivers pour identifier immédiatement les drivers à risque qui doivent être mis à jour ou désinstallés avant qu'un attaquant ne les exploite. Cette vérification doit être intégrée dans le processus d'audit trimestriel des endpoints des organisations françaises soumises aux exigences ANSSI ou NIS 2, et automatisée via Intune Proactive Remediation pour une surveillance continue et un rapport de conformité en temps réel disponible dans Endpoint Analytics.

```
 # Vérifier les drivers installés contre la liste LOLDrivers
$LOLHashes = @(
    "31f4cfb4c71da44120752721103a16512444c13c",  # gdrv.sys
    "74f96bc2e8c8fb1b1bf9a8b8f8c4dfd5e6a7b8c9",  # mhyprot2.sys
    "2b7c4d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c"   # rtcore64.sys
)
Get-ChildItem "$env:windir\system32\drivers\*.sys" -ErrorAction SilentlyContinue |
    ForEach-Object {
        $hash = (Get-FileHash $_.FullName -Algorithm SHA1).Hash.ToLower()
        if ($hash -in $LOLHashes) {
            Write-Warning "VULNERABLE DRIVER FOUND: $($_.Name) - Hash: $hash"
        }
    }
```

La méthodologie d'utilisation de LOLDrivers.io dans une équipe défensive commence par l'export régulier de la liste complète des drivers en format JSON depuis le repository GitHub officiel, puis la construction d'une base de données locale des hashs SHA256 et SHA1 de tous les drivers vulnérables répertoriés. Cette base locale est ensuite utilisée dans les règles Sigma de détection des SIEM, dans les scripts de vérification Intune Proactive Remediation, et dans les configurations Sysmon pour le filtrage des événements de chargement de drivers. La mise à jour hebdomadaire de cette base de données LOLDrivers locale est une pratique que toutes les équipes SOC des organisations françaises soumises aux exigences ANSSI devraient intégrer dans leurs processus de veille sur les menaces, au même titre que la surveillance des bulletins CERT-FR et des avis de sécurité Microsoft Patch Tuesday.

KASLR Bypass : contournement de la randomisation des adresses noyau

KASLR (Kernel Address Space Layout Randomization) randomise les adresses de base du noyau, des drivers kernel et des structures de données noyau à chaque démarrage, rendant difficile pour un attaquant de prédire l'emplacement en mémoire des fonctions et structures noyau qu'il cible. Sans la connaissance des adresses précises, il est impossible d'exploiter la majorité des vulnérabilités noyau ou de désactiver les protections de sécurité en modifiant des structures de données noyau spécifiques. KASLR est donc une défense importante mais

insuffisante seule, particulièrement face à un attaquant disposant d'une primitive de lecture mémoire arbitraire via un driver BYOVD.

KASLR sur Windows est contournable par plusieurs techniques documentées en 2026 : la primitive de lecture mémoire arbitraire fournie par un driver BYOVD permet de lire les structures noyau pour découvrir leurs adresses actuelles via le pattern scanning, la fuite d'adresses noyau via certains appels à `NtQuerySystemInformation` dans des contextes non restreints, et les attaques de timing sur les side-channels du cache processeur qui révèlent des informations sur les adresses en mémoire. La combinaison BYOVD (pour la primitive d'accès mémoire) + KASLR bypass (pour découvrir les adresses) est le pattern d'attaque dominant dans les incidents APT analysés en France en 2024 et 2025. Comprendre cette séquence d'attaque est indispensable pour concevoir des règles de détection comportementale qui identifient les patterns suspects avant que l'exploitation complète du noyau ne soit accomplie et que les protections ne soient désactivées de manière irréversible sans redémarrage du système.

Les mesures additionnelles de réduction de la surface d'attaque KASLR incluent la configuration de **Kernel CFG (Control Flow Guard)** qui restreint les cibles valides des sauts indirects en mémoire noyau, empêchant les techniques de ROP (Return Oriented Programming) utilisées pour construire des chaînes d'exploitation arbitraires à partir de gadgets noyau existants après un bypass KASLR réussi. La restriction des appels `NtQuerySystemInformation` via les politiques de restriction des appels système (syscall filtering) disponibles dans Windows 11 via les mécanismes de restriction des processus réduit également la surface d'exploitation KASLR disponible en user mode. Ces mesures combinées créent un environnement où même un attaquant disposant d'un driver BYOVD valide doit surmonter de nombreux obstacles supplémentaires avant d'obtenir l'exécution arbitraire de code en Ring 0 sur un système Windows 11 correctement durci selon les recommandations ANSSI.

HVCI : Hypervisor-Protected Code Integrity — la contre-mesure principale

HVCI (Hypervisor-Protected Code Integrity), aussi appelé Memory Integrity dans les paramètres Windows Security, est la contre-mesure la plus efficace contre les attaques BYOVD et l'exploitation kernel en général. HVCI utilise la virtualisation matérielle (Hyper-V VBS) pour

isoler le code de vérification de l'intégrité dans un Secure World séparé du noyau Windows, empêchant toute modification des protections d'intégrité même depuis le Ring 0. Avec HVCI actif, le système refuse de charger tout driver ou code noyau non signé avec un certificat valide de la chaîne de confiance Microsoft, rendant BYOVD largement inefficace car même un driver signé ne peut exécuter de code non autorisé via sa vulnérabilité.

L'activation de HVCI nécessite du matériel compatible (processeur avec virtualisation, IOMMU, TPM 2.0) et peut impacter les performances de 2 à 10% selon les charges de travail. Cet impact est acceptable pour les postes professionnels modernes mais peut être problématique sur des serveurs de calcul intensif. La documentation Microsoft HVCI détaille la procédure d'activation via Intune, GPO, ou les paramètres Windows Security. L'ANSSI recommande d'activer HVCI sur tous les postes Windows 11 dans les organisations OIV et OSE, et sa vérification est incluse dans les critères d'évaluation lors des contrôles de conformité ANSSI. Mon opinion est ferme : toute organisation qui ne déploie pas HVCI sur ses endpoints en 2026 laisse une fenêtre d'exploitation majeure ouverte que les groupes APT savent parfaitement exploiter via BYOVD, et cette négligence sera inévitablement un facteur aggravant lors d'une compromission et d'une notification à l'ANSSI.

Vulnerable Driver Blocklist : la liste noire Microsoft des drivers dangereux

La **Vulnerable Driver Blocklist** est une liste noire maintenue par Microsoft de drivers Windows connus pour être vulnérables à l'exploitation BYOVD ou utilisés activement dans des attaques. Intégrée dans Windows Defender Application Control (WDAC) et activée automatiquement sur Windows 11 22H2+ lorsque HVCI est actif, la blocklist empêche le chargement de ces drivers dans le noyau Windows même si l'attaquant les introduit physiquement sur le système. La blocklist est mise à jour mensuellement par Microsoft et synchronisée via Windows Update, avec publication des nouvelles entrées dans le repository GitHub Microsoft WDAC.

Les organisations gérant leur propre politique WDAC personnalisée doivent intégrer la Vulnerable Driver Blocklist Microsoft comme baseline obligatoire, en plus de leurs règles applicatives spécifiques. La dérogation à cette baseline — par exemple pour maintenir un logiciel utilisant un driver sur la blocklist — nécessite une justification écrite et une mesure de

compensation appropriée (isolation réseau du système, surveillance renforcée). Le référentiel GitHub Microsoft WDAC publie les mises à jour de la blocklist avec les nouveaux drivers bloqués et les CVE associées pour chaque cycle de mise à jour mensuel.

Driver BYOVD	CVE	Groupes utilisateurs	Capacité d'exploitation
gdrv.sys (Gigabyte)	CVE-2018-19320	BlackByte, Scattered Spider	R/W mémoire arbitraire
mhyprot2.sys (miHoYo)	Non CVE	Groupes ransomware 2023-2024	Kill processus Ring 0
rtcore64.sys (MSI)	CVE-2019-16098	APT41, divers	R/W registres MSR
dbutil_2_3.sys (Dell)	CVE-2021-21551	Multiple 2021-2023	R/W mémoire physique
ene.sys (ENE Tech)	CVE-2022-42455	Wipers APT	Accès mémoire physique
speedfan.sys (Almico)	Non CVE	PoC publics	I/O ports, PCI

PPL Bypass : contourner la protection des processus LSASS et EDR

PPL (Protected Process Light) est une fonctionnalité Windows qui protège les processus sensibles comme LSASS (qui stocke les credentials Windows en mémoire) et les agents EDR contre l'injection de code et l'accès direct à leur espace mémoire depuis des processus non-PPL. Un processus PPL ne peut être lu, modifié ou terminé que par d'autres processus avec un niveau PPL égal ou supérieur, empêchant les attaquants d'extraire les credentials via Mimikatz ou de désactiver les EDR depuis le user mode.

Les techniques de bypass PPL documentées en 2026 exploitent toutes une capacité d'écriture mémoire noyau, généralement via un driver BYOVD : la modification du champ `PS_PROTECTION` dans la structure EPROCESS du processus PPL cible pour abaisser son niveau de protection à zéro, permettant ensuite l'injection depuis un processus user-mode standard. Ce bypass PPL via BYOVD est utilisé par les malwares EDR-killer comme AuKill, Terminator, et Spyboy Terminator, documentés dans de nombreuses campagnes ransomware de 2023 et 2024 ciblant des organisations françaises. La défense contre ces EDR-killers passe par l'activation de HVCI

qui empêche la modification des structures EPROCESS via un driver vulnérable en validant chaque écriture mémoire noyau dans le Secure World de VBS avant qu'elle ne soit appliquée au niveau du hardware, rendant le bypass PPL physiquement impossible même avec un driver BYOVD valide.

Le monitoring des tentatives de bypass PPL s'effectue via l'Event ID 4656 (tentative d'accès à un objet) avec les flags d'accès PROCESS_TERMINATE ou PROCESS_VM_WRITE sur des processus PPL comme LSASS (PID variable, mais identifiable via le nom d'image lsass.exe), ainsi que via les événements Sysmon Event ID 10 (ProcessAccess) qui journalisent les tentatives d'accès à la mémoire d'un processus avec des masques de droits d'accès suspects. Une alerte Sentinel sur un accès PROCESS_VM_WRITE à lsass.exe depuis un processus non-PPL doit être considérée comme un indicateur d'attaque critique nécessitant une réponse immédiate, même si l'accès a été bloqué par les protections PPL actives, car cela indique qu'un attaquant tente activement de dumper les credentials en mémoire sur ce système spécifique.

Kernel Data Protection (KDP) : protéger les structures de données noyau

Kernel Data Protection (KDP), introduit dans Windows 10 version 2004, utilise la virtualisation hardware pour protéger certaines régions de mémoire noyau en lecture seule, empêchant toute modification même depuis le Ring 0. Les structures protégées par KDP incluent les données de configuration noyau, les politiques de sécurité, et les informations d'intégrité des drivers. Quand un driver BYOVD tente de modifier ces structures protégées pour contourner les mécanismes de sécurité, le système génère une exception matérielle qui stoppe l'opération avant qu'elle ne produise son effet.

L'activation de KDP est automatique lorsque HVCI est actif sur un système Windows 10 20H1 ou supérieur. Les deux mécanismes ensemble créent une couche de défense en profondeur significativement plus difficile à contourner que chaque protection individuellement, même pour des attaquants disposant d'un driver BYOVD valide avec une primitive d'écriture mémoire noyau. Microsoft continue d'étendre la couverture de KDP à de nouvelles structures noyau dans chaque mise à jour majeure de Windows 10 et Windows 11, élargissant progressivement la protection contre les techniques d'exploitation kernel avancées utilisées par les groupes APT les

plus sophistiqués. La vérification de l'état KDP sur le parc s'effectue via la même commande PowerShell que HVCI, les deux mécanismes étant intrinsèquement liés dans l'implémentation Windows et ne pouvant pas être activés indépendamment l'un de l'autre dans les configurations de production actuelles.

WDAC : déploiement des politiques de contrôle des drivers kernel

Windows Defender Application Control (WDAC) est la solution de contrôle applicatif Microsoft permettant de définir quels exécutables et drivers peuvent s'exécuter sur les systèmes Windows gérés. Pour la défense contre BYOVD, WDAC déploie la Vulnerable Driver Blocklist sur l'ensemble du parc et implémente des politiques de signature strictes n'autorisant que les drivers ayant un certificat WHQL valide fourni par des éditeurs approuvés. La différence clé avec AppLocker (solution historique) est que WDAC couvre les drivers kernel (fichiers .sys) que AppLocker ne supporte pas — WDAC est donc le seul outil Microsoft capable de bloquer le chargement de drivers BYOVD de manière préventive avant toute tentative d'exploitation.

```
 # Déploiement WDAC Vulnerable Driver Blocklist via PowerShell
$blocklistUrl = "https://aka.ms/VulnerableDriverBlockList"
$policyPath = "$env:TEMP\SiPolicy.p7b"
Invoke-WebRequest -Uri $blocklistUrl -OutFile $policyPath
# Déployer via CiTool (Windows 11 22H2+)
CiTool --update-policy $policyPath --json
# Ou via chemin système traditionnel (nécessite redémarrage)
Copy-Item $policyPath "$env:windir\System32\CodeIntegrity\SiPolicy.p7b"
# Vérifier l'état de la politique WDAC
CiTool --list-policies
```

Ce script déploie la blocklist officielle Microsoft sur un système cible. Dans un environnement Intune, cette opération est automatisable via un script de remédiation déployé sur l'ensemble du parc en quelques heures. La vérification post-déploiement via `CiTool --list-policies` confirme que la politique est active et retourne l'identifiant unique de la politique déployée. Le suivi de la conformité WDAC sur l'ensemble du parc est visible dans le rapport de configuration des appareils Intune sous l'onglet Device configuration, permettant d'identifier les systèmes où le déploiement a échoué et de les remettre en conformité en priorité.

Détection des attaques BYOVD : Sysmon et requêtes KQL pour Sentinel

La détection des attaques BYOVD repose sur la surveillance du chargement de drivers kernel via Sysmon Event ID 6 (Driver loaded), qui enregistre chaque driver chargé avec son chemin, son hash SHA256, sa signature et son signataire. Une règle analytique Sentinel qui compare les drivers chargés avec la liste des hashs LOLDrivers connus permet d'identifier en temps réel l'utilisation d'un driver BYOVD sur les endpoints. Cette règle doit être couplée avec une alerte critique déclenchant une investigation immédiate, car le chargement d'un driver BYOVD connu indique presque certainement une attaque en cours ou imminente nécessitant une isolation immédiate du système concerné avant que l'attaquant ne désactive les protections EDR.

```
// Hunting BYOVD — Sysmon Event ID 6 — Microsoft Sentinel KQL
let VulnerableDriverHashes = datatable(SHA256Hash:string, DriverName:string) [
    "2b7c4d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d", "gdrv.sys",
    "3c8d5e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e", "mhyprot2.sys"
];
Event
| where TimeGenerated > ago(24h) and Source == "Microsoft-Windows-Sysmon" and EventID == 6
| extend Hash = extract(@"Hashes:[^
]*SHA256=([A-Fa-f0-9]+)", 1, RenderedDescription)
| extend DriverPath = extract(@"ImageLoaded: (.+)", 1, RenderedDescription)
| join kind=inner VulnerableDriverHashes on $left.Hash == $right.SHA256Hash
| project TimeGenerated, Computer, DriverPath, DriverName, Hash
| order by TimeGenerated desc
```

EDR et sécurité noyau : la course aux armements permanente

Les solutions EDR modernes s'appuient massivement sur des hooks noyau pour intercepter les appels système suspects et détecter les comportements malveillants. Cette dépendance au Ring 0 pour la visibilité crée une vulnérabilité structurelle : un attaquant obtenant l'exécution de code Ring 0 via BYOVD peut supprimer ces hooks, rendant l'EDR aveugle. C'est précisément cette capacité "EDR killer" qui rend les drivers BYOVD si précieux dans les arsenaux des groupes

ransomware avancés comme ALPHV/BlackCat, LockBit 3.0 et Cl0p, qui incluent systématiquement une phase de neutralisation des EDR avant le déploiement du chiffreur final.

La réponse des éditeurs EDR à cette menace passe par l'utilisation de PPL pour leurs processus agent, l'intégration avec HVCI pour protéger leurs hooks noyau via le Secure World de VBS, et des mécanismes de détection des tentatives de déchargement de leurs propres drivers. Microsoft Defender for Endpoint (MDE) intègre depuis 2023 une protection anti-tamper qui utilise HVCI pour rendre ses protections noyau immuables même face à un attaquant disposant de droits administrateur complets. Cette approche converge vers une architecture où la sécurité du noyau repose sur des mécanismes hardware plutôt que sur la fiabilité du logiciel noyau seul, une évolution fondamentale de l'architecture de sécurité Windows vers une défense ancrée dans le silicon et le firmware plutôt que dans le seul logiciel susceptible d'être modifié par un attaquant privilégié.

Bootkits et rootkits firmware : au-delà du noyau Windows

Les **bootkits** représentent une évolution encore plus dangereuse des attaques noyau : ils s'installent dans le secteur de démarrage (MBR/VBR) ou dans le firmware UEFI lui-même, s'exécutant avant que le noyau Windows ne démarre et donc avant que toute protection logicielle ne soit active. **BlackLotus**, découvert en octobre 2022 et analysé par ESET, a été le premier bootkit UEFI capable de contourner le Secure Boot sur Windows 11, en exploitant une vulnérabilité dans le chargeur de démarrage Windows (CVE-2022-21894). Ce malware a été utilisé dans des attaques ciblées contre des organisations gouvernementales et de défense européennes, avec des variantes analysées par le CERT-FR dans ses bulletins de 2023. Une fois installé dans le firmware UEFI, un bootkit survit aux réinstallations du système d'exploitation, aux remplacements du disque dur, et même aux tentatives de nettoyage par des outils de sécurité classiques qui n'ont pas accès au firmware.

La défense contre les bootkits firmware repose sur plusieurs mécanismes complémentaires : le **Secure Boot** vérifie la signature cryptographique du chargeur Windows avant de l'exécuter, empêchant les bootkits non signés de s'installer dans la chaîne de démarrage, **Trusted Boot** mesure l'intégrité du noyau et des drivers au démarrage et signale toute anomalie via le TPM, et

la fonctionnalité **UEFI Secure Boot Advanced Targeting (SBAT)** introduite en 2022 permet de révoquer les composants de démarrage vulnérables même s'ils sont encore signés par des certificats valides. Le patch de sécurité Microsoft pour CVE-2022-21894 (KB5012170) a mis à jour la base de données SBAT pour bloquer les chargeurs de démarrage vulnérables exploités par BlackLotus. L'application de ce patch est critique pour toutes les organisations soumises aux exigences ANSSI, et sa vérification doit être incluse dans les procédures d'audit de sécurité des endpoints. Notre service de sécurité technique inclut la vérification de la configuration Secure Boot et SBAT sur les endpoints critiques lors des audits de posture de sécurité.

La détection d'un bootkit UEFI déjà installé sur un système en production est extrêmement difficile depuis le système d'exploitation lui-même, car le bootkit s'exécute avant tout le code OS et peut intercepter les tentatives de vérification de son propre firmware. Les approches de détection incluent la vérification hors-ligne via un live CD ou un environnement WinPE de l'intégrité du firmware UEFI en le comparant avec une image de référence du fabricant, la surveillance des modifications dans les variables UEFI accessibles depuis Windows via l'API `GetFirmwareEnvironmentVariable`, et l'analyse des mesures TPM stockées dans les PCR (Platform Configuration Registers) qui révèlent des anomalies dans la chaîne de démarrage si un composant non autorisé a été exécuté avant Windows. Les organisations exposées aux menaces APT de niveau État devraient effectuer ces vérifications sur leurs systèmes les plus critiques au moins annuellement.

Patch Management des CVE noyau : priorités et délais ANSSI

Le patch management des vulnérabilités noyau Windows doit être traité avec une priorité maximale en raison de l'impact systémique potentiel d'une exploitation réussie en Ring 0. L'ANSSI recommande un délai de patch de 72 heures maximum pour les CVE noyau Windows activement exploitées, marquées dans le catalogue CISA KEV ou avec un score CVSS supérieur à 9.0, sur tous les systèmes sensibles OIV et OSE. Pour les CVE noyau non encore exploitées, le délai recommandé est de 30 jours, compatible avec le cycle de patch management mensuel aligné sur le Patch Tuesday Microsoft du deuxième mardi de chaque mois.

Les CVE noyau Windows les plus critiques de 2024 et 2025 incluent des vulnérabilités dans le Common Log File System Driver (CVE-2023-28252, exploitée par le groupe ALPHV pour déployer Nokoyawa ransomware), le Windows Win32k subsystem (CVE-2024-30051, utilisée dans des attaques ciblées en Europe), et le Windows Error Reporting Service (CVE-2024-29988). Ces vulnérabilités sont toutes liées à des élévations de privilèges depuis le user mode vers le Ring 0, démontrant que les voies d'exploitation kernel ne passent pas exclusivement par les drivers BYOVD mais aussi par des vulnérabilités dans les composants Windows natifs qui ne peuvent être mitigées que par l'application rapide des correctifs Microsoft via Windows Update for Business géré par Intune.

Microsoft Pluton et Secure Boot : sécurité hardware de nouvelle génération

Microsoft Pluton, disponible sur certains processeurs AMD et Intel depuis 2022 et natif sur les Snapdragon X Elite, est une puce de sécurité intégrée directement dans le CPU. Elle stocke les clés cryptographiques et les mécanismes de sécurité dans une région inaccessible même depuis le CPU principal, éliminant la surface d'attaque du bus de communication CPU-TPM externe (bus sniffing attacks documentées contre le TPM standard). Pour les organisations gérant des postes de travail de direction ou des systèmes d'information très sensibles, les appareils équipés de Microsoft Pluton représentent l'état de l'art en matière de sécurité hardware pour Windows en 2026.

La chaîne de démarrage sécurisé (**Secure Boot Chain**) étendue via Pluton couvre l'intégralité du processus de démarrage : depuis le firmware UEFI jusqu'au chargeur Windows, en passant par le TPM Pluton et le contrôleur de démarrage sécurisé. Toute modification non autorisée d'un composant de cette chaîne — firmware rootkit, bootkit, ou driver pré-OS malveillant — est détectée et bloque le démarrage avant que Windows ne charge, empêchant catégoriquement les attaques au niveau du firmware que BitLocker et HVCI seuls ne peuvent pas toujours contrecarrer. La certification Secured-core PC de Microsoft valide que les appareils respectent toutes ces exigences hardware de sécurité avancée et constitue un critère de sélection à intégrer dans les appels d'offres d'équipements informatiques pour les organisations les plus sensibles.

Forensics d'une attaque kernel : artefacts et investigation post-compromission

L'investigation forensique d'une attaque BYOVD après compromission repose sur l'analyse de plusieurs sources d'artefacts : les logs Windows System (Event ID 7045 pour les services et drivers nouvellement installés), les clés de registre `HKLM\SYSTEM\CurrentControlSet\Services` qui conservent les entrées de drivers même après suppression du fichier, les timestamps NTFS dans `C:\Windows\System32\drivers\` révélant les drivers inhabituels récemment introduits, et les logs Sysmon Event ID 6 si Sysmon était déployé avant l'incident. La présence d'un fichier .sys dans un répertoire temporaire ou dans un chemin inhabituel est un indicateur fort d'une tentative BYOVD qui doit déclencher une investigation immédiate.

L'analyse de la mémoire RAM via des outils comme **WinPmem** (dump mémoire) combiné avec **Volatility 3** et ses plugins Windows spécifiques permet de retrouver les structures noyau modifiées par le driver BYOVD, y compris les modifications de la table SSDT (System Service Descriptor Table) pour les hooks noyau et les modifications des champs `PS_PROTECTION` des processus pour les attaques PPL bypass. Cette analyse mémoire doit être réalisée idéalement avant le redémarrage du système compromis, car la mémoire volatile est perdue au redémarrage et avec elle les traces les plus fiables de l'exploitation noyau. Les équipes SOC doivent avoir un runbook documenté pour le triage forensique des incidents d'exploitation kernel, incluant les commandes de capture mémoire et les plugins Volatility pertinents pour Windows 10 et Windows 11 qui diffèrent légèrement dans leurs structures internes et nécessitent des profils de symboles spécifiques à chaque version.

Red Team et tests d'exploitation kernel : méthodologie et éthique

Les tests d'exploitation kernel dans le cadre d'exercices Red Team autorisés permettent de valider l'efficacité des contre-mesures déployées (HVCI, WDAC, PPL) avant qu'un vrai attaquant ne les teste en production. Ces tests incluent typiquement : tentative de chargement d'un driver BYOVD depuis la liste LOLDrivers pour vérifier que WDAC et la Vulnerable Driver Blocklist les bloquent effectivement, tentative de désactivation du PPL de l'agent EDR pour valider la

protection anti-tamper, et tentative d'exploitation d'une CVE noyau sur un environnement de test pour vérifier que le patch est bien appliqué et que les mécanismes de mitigation (KASLR, KDP) réduisent l'exploitabilité à un niveau acceptable.

Notre équipe Red Team propose des exercices de simulation d'attaque incluant des techniques BYOVD et d'escalade de privilèges noyau dans des environnements de test isolés, délivrant un rapport de recommandations conforme aux référentiels ANSSI et MITRE ATT&CK. Ces exercices sont accompagnés d'une session de remédiation guidée pour corriger les configurations défaillantes identifiées. Mon opinion est ferme sur ce point : toute organisation utilisant Windows dans un secteur réglementé devrait soumettre ses protections noyau à un test Red Team annuel, car c'est le seul moyen de confirmer que HVCI, WDAC et les protections PPL fonctionnent comme prévu dans votre configuration spécifique et non uniquement dans les environnements de laboratoire Microsoft qui bénéficient d'une configuration idéale rarement reproduite exactement en production.

Intégration SOC : alertes kernel dans Sentinel et playbooks de réponse

L'intégration des alertes d'exploitation kernel dans un programme SOC structuré nécessite des règles analytiques Sentinel spécifiques et des playbooks de réponse adaptés à la criticité de ces incidents. Une alerte de chargement d'un driver BYOVD connu doit être traitée comme un incident critique de niveau P1, car elle indique presque certainement une attaque active en cours : un attaquant dispose déjà de droits administrateur locaux sur l'endpoint cible et cherche à désactiver les protections EDR pour passer à l'étape suivante de son attaque, qu'il s'agisse d'un mouvement latéral vers d'autres systèmes, d'une exfiltration de données sensibles, ou du déploiement d'un ransomware sur l'ensemble du réseau.

Le playbook de réponse pour une alerte BYOVD confirmée doit inclure : isolation immédiate de l'endpoint du réseau via Intune Remote Actions ou via un segment VLAN de quarantaine automatisé, capture de la mémoire RAM de l'endpoint avant redémarrage pour l'analyse forensique ultérieure, review de toutes les connexions réseau sortantes de l'endpoint dans les 24 heures précédant l'alerte pour identifier les mouvements latéraux potentiels, et vérification des authentifications depuis l'identité de l'utilisateur de l'endpoint compromis dans Microsoft 365

pour détecter une utilisation des credentials volés depuis d'autres systèmes. Pour les organisations soumises à la notification obligatoire NIS 2, un incident d'exploitation kernel doit être considéré comme un incident significatif nécessitant une notification à l'ANSSI dans les 72 heures suivant la confirmation de la compromission.

Accompagnement sécurité kernel : évaluation et plan de remédiation

L'évaluation de la posture de sécurité kernel Windows d'une organisation requiert une expertise technique rare et une connaissance actualisée des techniques d'attaque les plus récentes, combinant la compréhension de l'architecture x86-64, des mécanismes de protection Windows (HVCI, KDP, PPL), et des outils d'attaque documentés dans les incidents réels. Notre service de RSSI externalisé inclut une revue trimestrielle de la configuration HVCI, WDAC et de la Vulnerable Driver Blocklist sur les systèmes gérés, avec un rapport de conformité aux recommandations ANSSI et une priorisation des actions de remédiation selon le niveau d'exposition réel de chaque catégorie de systèmes dans l'organisation.

Pour les organisations qui doivent démontrer leur conformité aux exigences de sécurité dans le cadre de NIS 2 ou d'une certification ISO 27001, notre audit de sécurité technique approfondi couvre explicitement la configuration des protections kernel sur les endpoints critiques, avec vérification de l'état HVCI, de la présence de la Vulnerable Driver Blocklist dans les politiques WDAC, et de la configuration PPL pour les processus de sécurité. Contactez-nous via le diagnostic NIS 2 pour évaluer votre exposition actuelle aux techniques d'exploitation kernel et recevoir un plan de remédiation priorisé adapté à votre parc Windows et à votre secteur d'activité.

Questions fréquentes

HVCI est-il activé par défaut sur Windows 11 ?

HVCI est activé par défaut sur les nouveaux PC Windows 11 remplissant les prérequis matériels lors de la sortie de Windows 11 22H2. Sur les systèmes mis à niveau depuis Windows 10, HVCI peut ne pas être activé même si le matériel est compatible. Vérification via PowerShell : `(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).VirtualizationBasedSecurityStatus` doit retourner 2 pour confirmer que HVCI est actif et protégeant le système.

Quelle est la différence entre WDAC et AppLocker pour les drivers ?

AppLocker ne supporte pas le contrôle des drivers kernel (fichiers .sys) — il ne couvre que les exécutables user-mode. WDAC couvre à la fois les exécutables user-mode et les drivers kernel, avec une politique unifiée. Pour la défense contre BYOVD, seul WDAC peut bloquer le chargement de drivers vulnérables. Microsoft recommande de migrer vers WDAC pour tous les nouveaux déploiements de contrôle applicatif sur Windows 10 et 11.

Comment un attaquant charge-t-il un driver BYOVD sans droits admin ?

Le chargement d'un driver kernel requiert des droits administrateur locaux (SeLoadDriverPrivilege). Un attaquant sans droits admin doit d'abord obtenir des droits admin (élévation de privilèges via une CVE locale, accès avec des credentials volés) avant d'utiliser BYOVD. Le BYOVD est donc la deuxième phase d'une attaque, qui suit une phase initiale d'élévation de privilèges en user mode depuis un point d'entrée initial comme un phishing ou une exploitation de service exposé.

Comment détecter si un système est compromis via BYOVD après coup ?

Via plusieurs artefacts forensiques : Event Log System (Event ID 7045 pour les drivers nouvellement installés), clés de registre HKLM\SYSTEM\CurrentControlSet\Services

conservant les entrées même après suppression du fichier .sys, timestamps NTFS de fichiers .sys dans des chemins inhabituels, logs Sysmon Event ID 6 si configuré, et analyse mémoire RAM via WinPmem + Volatility 3 avant redémarrage pour identifier les structures noyau modifiées.

LOLDrivers recense-t-il tous les drivers vulnérables ?

Non. LOLDrivers.io est une ressource communautaire qui recense les vulnérabilités publiquement documentées. De nombreux drivers vulnérables non connus publiquement peuvent être exploités sans jamais apparaître dans les bases publiques. La défense basée uniquement sur la blocklist est insuffisante — elle doit être complétée par HVCI qui bloque tout code non autorisé en noyau, indépendamment de la liste de signatures bloquées.

Quelle est la recommandation ANSSI pour HVCI sur les systèmes sensibles ?

Le guide ANSSI 'Recommandations de sécurité relatives aux systèmes Windows' (2024) recommande d'activer HVCI (Memory Integrity) sur tous les systèmes Windows 10 et 11 des organisations OIV et OSE, sur les postes des administrateurs systèmes, et des utilisateurs manipulant des données sensibles. L'ANSSI considère HVCI comme une mesure de protection essentielle contre les techniques d'exploitation noyau avancées incluant BYOVD et les rootkits kernel.

Durcissement kernel Windows : plan d'action priorisé pour 2026

La sécurisation du noyau Windows contre les techniques d'exploitation avancées en 2026 repose sur trois piliers complémentaires : l'activation de **HVCI** (protection contre l'injection de code non autorisé en Ring 0), le déploiement de **WDAC avec la Vulnerable Driver Blocklist** (prévention du chargement de drivers BYOVD connus), et la configuration de **PPL** pour les processus de sécurité critiques comme LSASS et les agents EDR. Ces trois mesures, déployées via les politiques Intune MDM et les GPO Active Directory, créent une défense en profondeur qui rend les attaques BYOVD documentées largement inefficaces contre votre parc Windows.

Le plan d'action priorisé pour une organisation française soumise aux exigences ANSSI : (1) activer HVCI sur 100% des endpoints Windows 11 dans les 30 jours via Intune, (2) déployer la Vulnerable Driver Blocklist Microsoft via une politique WDAC dans les 15 jours, (3) activer la protection anti-tamper de l'EDR déployé dans les 7 jours, et (4) planifier un test Red Team annuel pour valider l'efficacité de l'ensemble de ces protections en conditions réelles. Notre équipe de tests d'intrusion peut accompagner chacune de ces étapes et fournir les rapports de conformité nécessaires pour vos audits ANSSI et NIS 2.