Attaques Firmware UEFI 2026 : Bootkits et Persistance Avancée

Points essentiels

- Les bootkits UEFI s'exécutent avant l'OS, échappant totalement aux antivirus et EDR
- BlackLotus (ESET, 2023) contourne Secure Boot sur Windows 11 entièrement à jour
- LoJax (APT28) et CosmicStrand visent des cibles stratégiques françaises et européennes
- CHIPSEC, TPM 2.0 et NIST SP 800-155 permettent de mesurer l'intégrité du firmware

À RETENIR

À retenir

Les bootkits UEFI s'exécutent avant l'OS, échappant totalement aux antivirus et EDR

BlackLotus (ESET, 2023) contourne Secure Boot sur Windows 11 entièrement à jour

LoJax (APT28) et CosmicStrand visent des cibles stratégiques françaises et européennes

CHIPSEC, TPM 2.0 et NIST SP 800-155 permettent de mesurer l'intégrité du firmware

Les **bootkits UEFI** constituent en 2026 l'une des menaces de persistance les plus redoutables des arsenaux offensifs, mobilisées aussi bien par les APT étatiques que par les groupes criminels les plus outillés. Là où un rootkit classique se contente d'opérer au niveau du système d'exploitation, ces implants s'ancrent dans le firmware de la carte mère ou dans la partition EFI du disque, c'est-à-dire en amont du chargement de Windows ou de Linux. Cette position privilégiée leur confère un contrôle total sur la chaîne de démarrage et une résistance quasi absolue au reformatage comme à la réinstallation. Comprendre le triptyque *uefi firmware bootkits persistance* devient dès lors indispensable pour toute équipe de défense : détection par attestation matérielle,

durcissement du Secure Boot et surveillance des mises à jour firmware forment aujourd'hui les seuls remparts crédibles.

> **Niveau de menace CERT-FR :** Les bootkits UEFI sont classifiés comme menaces de niveau critique par le CERT-FR depuis 2023. Plusieurs entités françaises des secteurs de la défense et de l'énergie ont été ciblées par des attaques utilisant des implants UEFI avec persistance à long terme.

Architecture UEFI : comprendre la chaîne de démarrage

L'UEFI (Unified Extensible Firmware Interface) est le successeur du BIOS traditionnel, standardisé par le consortium UEFI Alliance. Il gère l'initialisation du matériel et le chargement du bootloader système d'exploitation lors du démarrage. **La chaîne de démarrage UEFI suit une séquence précise** : initialisation du firmware UEFI depuis la mémoire flash SPI de la carte mère, exécution des phases Pre-EFI (PEI), Driver Execution Environment (DXE), et Boot Device Selection (BDS), puis chargement du bootloader depuis la partition EFI System Partition

(ESP) du disque. C'est dans ces étapes initiales que les bootkits s'insèrent pour obtenir une persistance avant le chargement du système d'exploitation.

L'ESP (EFI System Partition) est une partition FAT32 accessible depuis le système d'exploitation Windows ou Linux, typiquement montée sur /boot/efi ou accessible via des outils comme diskpart. Les fichiers bootloader légitimes (bootmgfw.efi pour Windows, grubx64.efi pour Linux) sont stockés dans cette partition et signés cryptographiquement. Secure Boot vérifie ces signatures avant l'exécution. Les bootkits peuvent cibler soit le firmware UEFI lui-même dans la mémoire flash SPI (persistance firmware, survit au remplacement du disque), soit les fichiers EFI dans l'ESP (plus accessible mais moins persistant). Les implications de cette distinction architecturale sont cruciales pour la remédiation : un bootkit dans l'ESP peut être éliminé en réinstallant le système d'exploitation, tandis qu'un bootkit dans le firmware UEFI nécessite un reflashage du firmware de la carte mère ou, dans les cas les plus graves, le remplacement de la carte mère elle-même.

BlackLotus : le bootkit qui a changé les règles du jeu

BlackLotus, analysé par ESET en mars 2023, est le premier bootkit UEFI public capable de bypasser Secure Boot sur des systèmes Windows 11 entièrement à jour, représentant une avancée technique majeure dans la menace bootkit. **Son mécanisme de bypass Secure Boot exploite la CVE-2022-21894 (baton.drop), une vulnérabilité dans le bootloader Windows qui permet de charger un bootloader non signé ou révoqué** si on peut amener le système à croire que le mode bootkit légitime est actif. Microsoft a patché cette vulnérabilité en janvier 2022, mais la mise à jour de la liste de révocation UEFI DB/DBx est un processus distinct du patch Windows qui nécessite une action explicite et qui, pour des raisons de compatibilité avec les systèmes de double-boot, n'a pas été déployée automatiquement.

⚡ Retour terrain

Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

BlackLotus est distribué en tant que kit commercial dans les forums cybercriminels russes (prix initial : 5 000 dollars US), ce qui indique sa sophistication — des bootkits d'une telle complexité technique nécessitent un investissement de développement considérable — mais aussi sa démocratisation au-delà des acteurs étatiques. Le malware installe un pilote Windows signé (via un certificat volé ou un driver vulnérable BYOVD), désactive HVCI (Hypervisor-Protected Code Integrity) et Windows Defender, établit une persistance UEFI via l'ESP, et établit des communications C2 via HTTPS. La désinfection de BlackLotus nécessite un reflashage complet de l'ESP et une vérification du firmware UEFI — impossible à réaliser avec les outils antivirus standard.

Bootkit	Découverte	Attribution	Vecteur UEFI	Survit au formatage
BlackLotus	2022-2023	Criminel (RU)	ESP + Secure Boot bypass	Non (ESP)
CosmicStrand	2022	APT chinois	Firmware SPI flash	Oui (firmware)
LoJax	2018	APT28 (RU)	Firmware SPI flash	Oui (firmware)
MosaicRegressor	2020	APT chinois	Firmware SPI flash	Oui (firmware)
ESPecter	2021	Inconnu	Partition ESP	Non (ESP)
ThunderStrike	2014	PoC (Trammell Hudson)	Option ROM Thunderbolt	Oui (firmware)

CosmicStrand : persistance firmware chinoise

CosmicStrand, analysé par Kaspersky en 2022 et attribué à un acteur APT chinois non nommé (probablement lié aux groupes opérant pour le Ministère de la Sécurité d'État), représente l'état de l'art des bootkits firmware en 2022-2026. Contrairement à BlackLotus qui opère dans l'ESP, **CosmicStrand s'implante directement dans le firmware UEFI de la carte mère en modifiant les images SPI flash, survivant ainsi à tout réinstallation du système d'exploitation, tout formatage de disque, et même au remplacement du disque dur.** La seule remédiation est le reflashage du firmware depuis une image officielle et vérifiée du fabricant.

CosmicStrand cible des cartes mères Gigabyte et Asus H81 (chipset Intel), populaires dans les environnements d'entreprise et gouvernementaux. Il injecte un shell code dans le DXE driver du firmware UEFI qui s'exécute avant Windows et installe un rootkit noyau Windows lors de chaque démarrage. Ce rootkit noyau télécharge ensuite un payload final depuis l'internet (infrastructure C2), permettant à l'attaquant de maintenir un accès persistant indépendamment des réinstallations du système. La sophistication requise pour développer un implant firmware aussi stable et discret — qui n'a pas crashé une seule des machines ciblées pendant des années — indique clairement des ressources étatiques de haut niveau.

Secure Boot : mécanismes et vecteurs de bypass

Secure Boot est un mécanisme UEFI qui vérifie la signature cryptographique de chaque composant chargé dans la chaîne de démarrage — bootloader, pilotes UEFI, noyau OS — avant son exécution. Les signatures valides sont définies dans une base de données (DB) stockée dans la mémoire NVRAM non volatile de la carte mère, et les signatures révoquées dans une liste de refus (DBx). **Secure Boot, correctement configuré, empêche le chargement de bootloaders ou de pilotes non signés, rendant les bootkits qui modifient les fichiers EFI de l'ESP inefficaces.**

Plusieurs techniques de bypass de Secure Boot ont été documentées. Le BYOVD (Bring Your Own Vulnerable Driver) exploite des pilotes Windows légitimement signés contenant des

vulnérabilités permettant l'exécution de code en mode noyau — plus de 200 pilotes vulnérables ont été documentés dans la liste du projet LOLDrivers. Une fois un code arbitraire en mode noyau, il est possible de désactiver Secure Boot en modifiant les variables NVRAM UEFI ou en utilisant des exploits kernel pour forcer le chargement de modules non signés. La CVE-2022-21894 exploitée par BlackLotus exploite une faille dans le bootloader Windows lui-même qui permet de court-circuiter la validation Secure Boot. La mise à jour de la liste DBx Microsoft pour inclure les certificats révoqués est la contre-mesure principale, mais cette mise à jour est optionnelle et n'est pas déployée automatiquement pour éviter des problèmes de compatibilité avec des systèmes legacy.

```
 # Vérifier l'état de Secure Boot sur Windows
# Via PowerShell
Confirm-SecureBootUEFI  # True si Secure Boot actif et validé

# Vérifier la DB/DBx (liste de révocation UEFI)
Get-SecureBootUEFI -Name db  # Base de données des certificats autorisés
Get-SecureBootUEFI -Name dbx  # Base de données des révocations

# Vérifier si la DBx Microsoft 2023 est appliquée
# (Protection contre BlackLotus et CVE-2022-21894)
$dbx = (Get-SecureBootUEFI -Name dbx).Bytes
if ($dbx.Length -gt 0x2000) { Write-Host "DBx mise a jour (OK)" } else { Write-Host "DBx ob

# Sur Linux : vérifier Secure Boot
mokutil --sb-state
# Secure Boot enabled = protégé
# Secure Boot disabled = vulnérable aux bootkits ESP

# Lister les clés Secure Boot enregistrées
mokutil --list-enrolled  # Clés MOK (Machine Owner Key)
efi-readvar -v db        # Clés DB UEFI
```

TPM 2.0 et attestation de l'intégrité du démarrage

Le Trusted Platform Module (TPM 2.0) est un composant matériel cryptographique qui mesure et enregistre l'intégrité de chaque étape de la chaîne de démarrage dans des registres PCR

(Platform Configuration Registers). Ces mesures, incluant le firmware UEFI, les variables NVRAM, le secteur de démarrage, le bootloader et le noyau OS, forment une "empreinte" cryptographique du processus de démarrage. **Si un bootkit modifie un composant de la chaîne de démarrage, les mesures PCR changent, permettant la détection de l'altération.**

L'attestation TPM permet à un serveur de vérification de distance de confirmer que le système a démarré avec un firmware et un système d'exploitation intègres et non modifiés. Microsoft Autopilot et les solutions MDM modernes utilisent l'attestation TPM pour vérifier l'intégrité des Windows 11 Secured-Core PCs avant de leur accorder l'accès aux ressources d'entreprise. BitLocker utilise le TPM pour lier le déchiffrement du volume à un état de démarrage spécifique — si le firmware UEFI est modifié par un bootkit, BitLocker détecte le changement de mesures PCR et refuse le déchiffrement automatique, forçant la saisie manuelle de la clé de récupération et alertant ainsi l'utilisateur d'une modification suspecte. Cette protection n'est efficace que si BitLocker est configuré avec TPM uniquement (sans PIN de pré-démarrage) et si les seuils de mesure PCR incluent les variables NVRAM UEFI critiques.

CHIPSEC : audit du firmware UEFI et des configurations matérielles

CHIPSEC est un outil open source développé par Intel permettant d'analyser la sécurité du firmware UEFI et des configurations matérielles. **CHIPSEC peut détecter des modifications non autorisées du firmware UEFI, des configurations SPI incorrectes permettant l'écriture non protégée dans la flash, des pilotes UEFI suspects chargés en mémoire, et des bootkits connus via des signatures intégrées.** Il s'exécute depuis un système d'exploitation live (Linux live USB) ou depuis le système en cours d'exécution et produit un rapport détaillé des anomalies détectées.

Les organisations gérant des actifs critiques (serveurs de production, postes administrateurs, systèmes OT connectés) devraient exécuter CHIPSEC lors de l'inventaire initial des équipements et périodiquement (tous les trimestres) pour détecter d'éventuelles modifications de firmware. La comparaison des hashs de firmware mesurés par CHIPSEC avec les images officielles du fabricant est le test le plus robuste pour détecter une persistance firmware. Cette approche est recommandée dans le guide NIST SP 800-155 (BIOS Integrity Measurement Guidelines) que

l'ANSSI a adapté dans ses recommandations sur la sécurité des systèmes industriels critiques (ICS/SCADA) où la persistance firmware est une menace particulièrement sérieuse.

```
 # Audit UEFI avec CHIPSEC
# Installation (Linux)
git clone https://github.com/chipsec/chipsec
cd chipsec && python setup.py install

# Exécuter tous les modules de sécurité UEFI
python chipsec_main.py --log chipsec_report.txt

# Modules spécifiques critiques
# Vérifier que SPI flash est protégée en écriture
python chipsec_main.py -m common.spi_write_protection

# Vérifier les protections mémoire UEFI
python chipsec_main.py -m common.smm_code_chk

# Vérifier les configurations Secure Boot
python chipsec_main.py -m common.secureboot.variables

# Extraire le firmware UEFI pour analyse hors-ligne
python chipsec_util.py spi dump firmware.bin
# Comparer avec l'image officielle du fabricant
sha256sum firmware.bin
# Puis comparer avec le hash officiel du fabricant
```

BYOVD (Bring Your Own Vulnerable Driver) : vecteur d'accès ring-0

BYOVD est une technique d'attaque où un attaquant charge un pilote Windows légitime mais vulnérable (ayant une signature Microsoft valide) pour exploiter ses vulnérabilités et obtenir un accès en mode noyau (ring-0). En 2026, la liste LOLDrivers recense plus de 200 pilotes Windows signés contenant des vulnérabilités connues permettant l'exécution de code arbitraire en mode noyau. **Ces pilotes proviennent d'éditeurs légitimes — fabricants de matériel, outils d'overclock, logiciels de diagnostic — qui ont signé des pilotes contenant des vulnérabilités non patchées il y a parfois des années.**

En mode noyau, un attaquant peut désactiver Windows Defender et tout EDR en terminant leurs processus protégés ou en modifiant leurs callbacks noyau, charger du code non signé en mémoire, contourner Secure Boot en modifiant les politiques de chargement en runtime, et installer un bootkit dans l'ESP ou même tenter de modifier le firmware UEFI si la protection d'écriture SPI est désactivée. Microsoft maintient une liste DBx (UEFI Revocation List) incluant les pilotes vulnérables connus, mais la mise à jour de cette liste sur les systèmes existants nécessite une action manuelle ou via Windows Update avec les bons paramètres. En 2026, HVCI (Hypervisor-Protected Code Integrity), activé par défaut sur Windows 11 Secured-Core PCs, bloque efficacement BYOVD en empêchant le chargement de pilotes non signés ou révoqués même depuis le mode noyau.

NIST SP 800-155 et la mesure d'intégrité du BIOS/UEFI

Le NIST SP 800-155 "BIOS Integrity Measurement Guidelines" fournit un framework pour mesurer et vérifier l'intégrité du firmware des systèmes informatiques dans les environnements gouvernementaux et critiques. **Ce standard définit une architecture de mesure basée sur le TPM et des protocoles d'attestation standardisés (TCG Attestation Protocol) permettant à des systèmes de gestion centraux de vérifier l'intégrité du firmware de tous les équipements du parc informatique.**

En France, l'ANSSI s'inspire de ces standards dans ses recommandations sur la sécurité des systèmes critiques (guides ANSSI pour les OES et les administrations). Les organisations gérant des systèmes classifiés ou sensibles sont encouragées à implémenter des mécanismes de mesure d'intégrité firmware basés sur le TPM, intégrés dans les processus de gestion des actifs. Les solutions commerciales de firmware security management comme HP Sure Start, Dell SafeBIOS et Lenovo ThinkShield implémentent des protections au-delà du standard UEFI Secure Boot standard, incluant la détection d'anomalies firmware par ML et la récupération automatique depuis des états protégés en mémoire ROM inaltérable. Ces fonctionnalités doivent être incluses dans les critères de sélection des équipements pour les postes sensibles et les serveurs critiques des organisations françaises.

Retour terrain : LoJax retrouvé dans une ambassade

La découverte de LoJax par ESET en 2018 reste l'un des cas les plus frappants de compromission firmware documentée publiquement. L'implant, attribué à APT28 (Fancy Bear, GRU russe), a été retrouvé dans le firmware UEFI d'un ordinateur utilisé dans un environnement diplomatique d'Europe de l'Est. La victime avait réinstallé Windows, remplacé le disque dur, et fait certifier le poste "propre" par ses équipes IT — sans jamais détecter que le malware résidait dans la mémoire flash SPI de la carte mère, immune à toute opération logicielle. La seule chose qui a permis la détection finale est l'exécution de CHIPSEC par une équipe de réponse à incident ESET lors d'une investigation approfondie suite à un comportement réseau anormal persistant. La leçon est claire : sans audit firmware spécifique, une compromission UEFI peut rester indétectable indéfiniment, même après des mesures de remédiation que l'équipe IT estime exhaustives.

HVCI et Secured-Core PC : la défense Microsoft

Microsoft a introduit la certification "Secured-Core PC" en 2019 pour les systèmes offrant une protection matérielle avancée contre les bootkits et les rootkits firmware. **Les Secured-Core PCs activent HVCI (Hypervisor-Protected Code Integrity), protègent le firmware de la modification via DRTM (Dynamic Root of Trust for Measurement), et utilisent le TPM 2.0 pour l'attestation d'intégrité du démarrage.** Windows 11 active automatiquement HVCI sur les matériels compatibles.

HVCI utilise la virtualisation matérielle (Intel VT-x/AMD-V) pour créer une couche hyperviseur qui protège l'intégrité du code en mode noyau Windows. Tous les pilotes noyau doivent passer par un processus de validation de signature avant exécution, même une fois en mode noyau. Cela bloque efficacement BYOVD — même un attaquant ayant exploité une vulnérabilité kernel pour accéder au ring-0 ne peut pas charger de code non signé supplémentaire car HVCI vérifie chaque page mémoire avant exécution. Pour les organisations gérant des postes sensibles, la migration

vers des Secured-Core PCs avec HVCI, TPM 2.0, et BitLocker avec mesures PCR UEFI représente la défense la plus robuste disponible commercialement contre les bootkits en 2026.

Détection des bootkits UEFI : méthodes et outils

La détection des bootkits UEFI est particulièrement difficile car ces malwares opèrent sous les systèmes de sécurité traditionnels. Plusieurs approches complémentaires permettent leur détection. **L'analyse des logs d'événements Windows** peut révéler des indicateurs indirects : erreurs de validation de signature pendant le démarrage, modifications des variables UEFI NVRAM enregistrées dans les logs système, ou chargement de pilotes non attendus en mémoire. Les EDR comme Microsoft Defender for Endpoint surveillent ces événements et peuvent alerter sur des patterns d'initialisation système anormaux.

L'analyse comparative du firmware est la méthode la plus fiable : extraire le firmware actuel avec CHIPSEC ou des outils fabricants, calculer son hash SHA256, et comparer avec l'image officielle du fabricant téléchargée depuis son site. Toute divergence indique une modification potentiellement malveillante. Pour les parcs de plusieurs milliers de machines, des solutions de firmware security management centralisées (HP Wolf Security, Dell SafeBIOS, Absolute Firmware) automatisent cette comparaison à l'échelle. Les solutions XDR (Extended Detection and Response) comme Microsoft Defender XDR intègrent en 2026 des capacités de détection de bootkits basées sur des signatures YARA de firmware et des anomalies de mesures TPM, permettant une détection plus rapide que les approches manuelles.

Remédiation d'une infection bootkit UEFI

La remédiation d'un bootkit UEFI dépend du type d'infection : ESP (partition EFI) ou firmware (mémoire flash SPI). **Pour un bootkit dans l'ESP :** booter depuis un live USB Linux, monter la partition ESP, supprimer les fichiers EFI suspects, réinstaller le bootloader Windows

(commandes `bcdboot` depuis le DVD d'installation Windows en mode récupération), vérifier l'état de Secure Boot, et activer HVCI après remédiation. **Pour un bootkit dans le firmware SPI :** le processus est beaucoup plus complexe — télécharger l'image firmware officielle du fabricant de la carte mère pour le modèle exact, utiliser les outils de reflashage du fabricant (Intel Flash Image Tool, ASUS EZ Flash, etc.) depuis un environnement bootable fiable (USB Live Linux), ou envoyer le matériel au fabricant pour reflashage en usine dans les cas les plus critiques.

Après toute remédiation d'infection UEFI, l'organisation doit vérifier et mettre à jour la liste DBx Microsoft via Windows Update avec l'option "Get updates for other Microsoft products" activée, activer HVCI et TPM 2.0 si pas encore fait, configurer BitLocker avec des mesures PCR couvrant les variables UEFI critiques, et auditer tous les autres systèmes du même modèle de carte mère pour s'assurer que l'infection n'a pas été répliquée. L'ANSSI recommande, pour les entités NIS 2 ayant subi une compromission firmware, une investigation forensique complète incluant l'analyse de tous les systèmes qui ont eu un contact réseau avec le système compromis pendant la période d'infection estimée.

Notre avis : les fabricants doivent faire plus pour sécuriser leur firmware

La sécurisation du firmware UEFI ne devrait pas reposer principalement sur les équipes de sécurité des organisations utilisatrices mais sur les fabricants de matériel eux-mêmes. **Trop de cartes mères et de PCs vendus en 2026 ne permettent pas d'activer HVCI, ont des implémentations Secure Boot défectueuses, ou ne proposent pas de mises à jour firmware régulières au-delà des deux premières années après commercialisation.** La pression réglementaire croissante — notamment le Cyber Resilience Act européen (CRA) qui impose des exigences de sécurité aux produits numériques vendus dans l'UE — devrait obliger les fabricants à améliorer la sécurité de leur firmware et à maintenir des mises à jour pendant au moins 5 ans après la fin de commercialisation. En attendant cette évolution, les RSSI des organisations critiques doivent inclure des critères de sécurité firmware stricts dans leurs appels d'offres matériels.

Mitigations recommandées NIST et Microsoft

Le NIST et Microsoft ont publié des recommandations détaillées pour se protéger contre les bootkits UEFI en 2023, directement en réponse à la divulgation de BlackLotus. Les mitigations prioritaires incluent l'application de la mise à jour KB5025885 (qui déploie la DBx mise à jour bloquant BlackLotus sur Windows 11 22H2+), l'activation de HVCI, l'activation de Secure Boot avec la DBx Microsoft la plus récente, la mise à jour du firmware UEFI vers la version la plus récente disponible pour chaque modèle de carte mère, et l'activation de BitLocker avec TPM uniquement en utilisant les PCR 7+11 qui couvrent les variables Secure Boot.

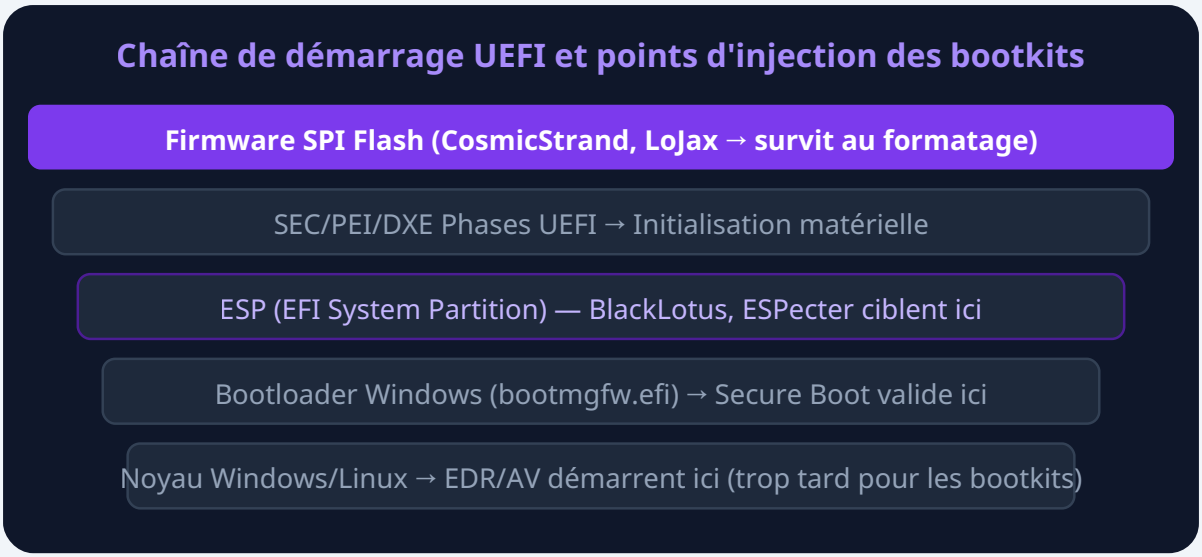
Défense	Protection contre	Implémentation	Priorité
Secure Boot + DBx mise à jour	Bootkits ESP, BlackLotus	KB5025885 + firmware update	P0
HVCI	BYOVD, code non signé kernel	Secured-Core PC ou config manuelle	P0
TPM 2.0 + BitLocker PCR 7	Modifications firmware/ bootloader	GPO BitLocker + TPM policy	P1
SPI write protection (hardware)	Bootkits firmware (CosmicStrand)	BIOS setup + CHIPSEC audit	P1
Firmware updates réguliers	Vulnérabilités UEFI connues	SCCM/MECM + Windows Update for Business	P1
CHIPSEC audit périodique	Infections firmware non détectées	Script automatisé live USB mensuel	P2

Sécurité de la supply chain firmware : risques fournisseurs

La supply chain du firmware UEFI est une surface d'attaque émergente préoccupante. Les firmwares UEFI des grandes marques (Dell, HP, Lenovo) sont développés à partir de bases de code communes (TianoCore EDK II) avec des contributions de multiples fournisseurs de

composants. **En 2022, des chercheurs de Binarly ont découvert plus de 23 vulnérabilités dans des firmwares UEFI de plusieurs fabricants majeurs utilisant le même code de référence — une illustration parfaite du risque de supply chain firmware.** Un attaquant ayant accès au processus de développement ou de distribution d'un firmware de grande marque pourrait potentiellement inclure un backdoor dans le firmware distribué à des millions de machines.

Les organisations critiques françaises (secteur défense, énergie, administrations) doivent inclure des exigences de sécurité de la supply chain firmware dans leurs contrats avec les fabricants d'équipements : vérification des chaînes de build firmware, tests de sécurité tiers des images firmware, et programmes de divulgation responsable pour les vulnérabilités firmware. Le Cyber Resilience Act européen, entré en vigueur en 2024, impose progressivement ces exigences aux fabricants vendant des produits numériques dans l'UE, avec des délais de conformité s'étalant jusqu'en 2027. Cette évolution réglementaire représente une avancée majeure pour la sécurité de la supply chain firmware, même si son impact pratique ne se fera sentir que progressivement au fil du renouvellement des parcs informatiques.



Articles connexes

UEFI Bootkits : techniques de persistance firmware avancées

Exploitation du noyau Windows : drivers et KASLR

Analyse malware 2026 : évasion de sandbox

Forensics IA : reconstruction post-hacking

Références officielles UEFI security

Les ressources de référence sur la sécurité UEFI incluent les travaux de CHIPSEC (Intel Open Source) pour l'audit firmware. Le NIST SP 800-155 "BIOS Integrity Measurement Guidelines" fournit le framework d'audit d'intégrité firmware pour les organisations gouvernementales. La base de données Eclypsium Firmware Threat Landscape recense les vulnérabilités firmware actives. Les analyses ESET des bootkits (BlackLotus, CosmicStrand, LoJax) restent les références techniques les plus détaillées disponibles publiquement.

Questions fréquentes sur les attaques UEFI et firmware

Secure Boot activé me protège-t-il complètement contre les bootkits UEFI ?

Secure Boot activé avec la base DBx Microsoft à jour offre une bonne protection contre les bootkits connus ciblant l'ESP comme BlackLotus. Mais Secure Boot ne protège pas contre les bootkits qui s'implantent directement dans le firmware SPI (CosmicStrand, LoJax), qui opèrent avant même la phase de vérification Secure Boot. Pour une protection complète, combinez Secure Boot avec HVCI, TPM 2.0 + BitLocker avec PCR 7, SPI write protection activée dans le BIOS setup, et des audits réguliers avec CHIPSEC.

Comment savoir si mon firmware UEFI a été compromis ?

Les signes indirects incluent : comportements système anormaux après une réinstallation complète du système d'exploitation, erreurs BitLocker "Trusted Platform Module has malfunctioned" récurrentes (signe de changement des mesures PCR), pilotes inconnus chargés en mémoire que vous ne pouvez pas désinstaller, et antivirus/EDR qui se désactivent mystérieusement au démarrage. La confirmation définitive nécessite l'exécution de CHIPSEC et la comparaison du hash du firmware extrait avec l'image officielle du fabricant de votre modèle exact de carte mère.

Un formatage du disque dur élimine-t-il un bootkit UEFI ?

Cela dépend du type de bootkit. Un bootkit dans l'ESP (comme BlackLotus ou ESPecter) est éliminé par un formatage complet et une réinstallation du système d'exploitation. Un bootkit dans le firmware SPI de la carte mère (CosmicStrand, LoJax, MosaicRegressor) survit à tout formatage de disque et même au remplacement du disque dur. La seule remédiation pour un bootkit firmware est le reflashage du firmware depuis une image officielle vérifiée du fabricant ou le remplacement physique de la carte mère.

À RETENIR

Points clés à retenir — UEFI Bootkits et Persistance Avancée 2026

Les bootkits UEFI opèrent avant le système d'exploitation — ils sont invisibles aux antivirus et EDR qui démarrent trop tard dans la chaîne de boot.

> **BlackLotus (2023) a démocratisé les bootkits** avec un bypass Secure Boot commercialisé à 5 000$ — la menace n'est plus réservée aux acteurs étatiques.
>
> **CosmicStrand et LoJax dans le firmware SPI** survivent au formatage du disque et nécessitent un reflashage firmware pour remédiation.
>
> **Secure Boot + DBx à jour (KB5025885) + HVCI** constituent la triade défensive minimum contre les bootkits ESP connus en 2026.
>
> **CHIPSEC** est l'outil open source de référence pour l'audit d'intégrité firmware — exécutable depuis un live USB Linux en 15 minutes.
>
> **TPM 2.0 + BitLocker avec PCR 7** détecte les modifications de la chaîne de boot en empêchant le déchiffrement automatique si les mesures changent.
>
> **Les Secured-Core PCs** avec HVCI et DRTM offrent la meilleure protection matérielle commercialement disponible contre les bootkits en 2026.

Outils open source de lecture et mise à jour firmware

En dehors de CHIPSEC, deux outils complémentaires constituent le socle de toute démarche d'audit firmware open source : *flashrom* et *fwupd*. Flashrom est un utilitaire en ligne de commande capable de lire, écrire et effacer le contenu des puces flash SPI qui stockent le firmware UEFI. Sur un système Linux, la commande `flashrom -p internal -r firmware_backup.bin` extrait le binaire complet du firmware en moins de deux minutes — à condition que le chipset Intel ME (Management Engine) n'ait pas verrouillé l'accès en lecture, ce qui est malheureusement le cas sur la majorité des laptops grand public depuis 2019. Sur les serveurs Dell iDRAC et HPE iLO, l'accès flashrom est souvent possible via le contrôleur de baseboard management (BMC), mais nécessite des privilèges root et une configuration BIOS préalable déverrouillant l'accès SPI. **La sauvegarde régulière du firmware via flashrom constitue le seul moyen fiable de détecter une modification de la puce SPI survenue entre deux audits CHIPSEC**, car la comparaison binaire entre le backup initial et le dump courant révèle toute altération, même d'un seul bit.

Fwupd est le daemon Linux de mise à jour firmware maintenu par Richard Hughes (Red Hat), désormais intégré par défaut dans Ubuntu, Fedora et Debian. Il s'appuie sur le protocole LVFS (Linux Vendor Firmware Service) pour distribuer les mises à jour firmware signées cryptographiquement par les fabricants. La commande `fwupdmgr get-updates` liste les mises à jour disponibles pour tous les composants du système — UEFI, contrôleurs NVMe, thunderbolt, processeurs EC — et `fwupdmgr update` les applique avec vérification de signature avant installation. Pour les équipes de sécurité, fwupd présente un avantage opérationnel majeur : son intégration dans les outils de gestion de configuration (Ansible, Chef) permet de centraliser et automatiser les mises à jour firmware au même titre que les patchs OS, comblant l'écart souvent constaté entre la rigueur du patch management OS et la négligence du firmware dans les organisations françaises.

Secure Boot sur Linux : GRUB, shim et les pièges de la chaîne

La chaîne Secure Boot sur les systèmes Linux est plus complexe qu'elle n'y paraît et présente des vecteurs d'attaque spécifiques que les équipes Blue Team doivent connaître. Sur une distribution majeure (Ubuntu, RHEL, Fedora), la chaîne de confiance UEFI fonctionne ainsi : le firmware UEFI charge le shim (un petit bootloader signé par Microsoft), qui charge GRUB (signé par le distributeur), qui charge le kernel (signé par le distributeur), avec à chaque étape une vérification de signature cryptographique. **La faiblesse historique de cette chaîne résidait dans le shim lui-même : CVE-2023-40547 (ShimBleed) permettait à un attaquant disposant d'un accès GRUB d'exécuter du code arbitraire avant le kernel**, contournant ainsi le GRUB Secure Boot bypass mitigation sans invalider la signature UEFI. Cette vulnérabilité, découverte en 2023, illustre que la chaîne Secure Boot est aussi solide que son maillon le plus faible — et que même des composants signés et dignes de confiance peuvent contenir des bugs exploitables en pre-OS.

Pour les organisations gérant des parcs Linux, la gestion du shim database (db, dbx) représente un défi opérationnel : quand un distributeur révoque une clé (ajout au dbx), les anciens bootloaders signés avec cette clé ne démarrent plus, ce qui peut bloquer des systèmes de récupération. La gestion de la Microsoft UEFI CA 2023 (qui remplace progressivement la UEFI CA 2011) nécessite des procédures de mise à jour coordonnées entre les équipes firmware, OS et

securité. L'outil `mokutil` (Machine Owner Key utility) permet de gérer les clés MOK — des clés personnalisées que les administrateurs peuvent ajouter à la chaîne Secure Boot sans passer par Microsoft — ce qui est pratique pour signer des kernels custom ou des modules non officiels, mais introduit un risque si un attaquant compromet la clé MOK privée stockée dans un vault non protégé.

Intégration de la détection firmware dans le SOC

La détection des compromissions firmware dans un SOC opérationnel requiert une approche différente des alertes de sécurité classiques, car les événements firmware sont rares, peu verbeux et difficiles à corréler avec des logs applicatifs. Plusieurs vecteurs de détection complémentaires doivent être activés pour constituer une couverture minimale. Premièrement, **l'intégration des logs Windows Event ID 1796 (Secure Boot policy) et 1800 (UEFI measured boot failure) dans le SIEM** permet d'alerter sur toute modification de la configuration Secure Boot ou tout échec de mesure PCR inattendu. Ces événements, enregistrés dans le journal système Windows, sont souvent ignorés car leur volume est quasi nul sur des parcs sains — mais leur apparition soudaine est un signal d'alarme majeur.

Deuxièmement, l'exploitation des attestations TPM via Windows Health Attestation Service (HAS) ou ses équivalents Linux (tpm2-tools + ima-evm-utils) permet de créer des rapports d'intégrité automatiques pour chaque machine du parc. En configurant un workflow d'attestation quotidien via Intune (Windows) ou Ansible (Linux), les équipes SOC reçoivent une alerte si la signature PCR d'une machine diverge de sa baseline enregistrée — ce qui signifie que quelque chose a changé dans la chaîne de boot, potentiellement un bootkit. Cette approche, dite de "remote attestation", est recommandée par le NIST SP 800-155 comme contrôle de détection de référence pour les environnements haute sécurité. En France, l'ANSSI recommande son déploiement dans les SI les plus sensibles (OIV, OSE) dans le cadre de son référentiel de sécurité des systèmes d'information.

Risque supply chain : les fabricants sous pression

L'écosystème UEFI repose sur une poignée d'acteurs dominants — AMI (American Megatrends), Phoenix Technologies et Insyde Software — qui fournissent le code UEFI de base (codebase IBB, Initial Boot Block) à la quasi-totalité des fabricants OEM mondiaux. Cette concentration crée un risque de supply chain systémique : une vulnérabilité dans le code AMI UEFI touche simultanément des centaines de modèles de serveurs et de laptops de marques différentes. La campagne PixieFail (CVE-2023-45229 à CVE-2023-45237) en est l'illustration parfaite : neuf vulnérabilités dans la stack réseau IPv6 de l'UEFI EDK2 (le code open source d'Intel utilisé comme base par AMI, Phoenix et Insyde) touchaient des serveurs Lenovo, Dell, HP, Intel, Microsoft (Hyper-V) et AMD simultanément.

Face à ce risque, les organisations françaises critiques doivent exiger contractuellement des SLA de mise à jour firmware de leurs fournisseurs hardware : délai maximum de 30 jours entre la publication d'un CVE firmware critique et la disponibilité d'une mise à jour signée, canal de notification prioritaire pour les vulnérabilités UEFI, et accès au code source UEFI sous NDA pour audit indépendant si nécessaire. Ces clauses contractuelles, rares en 2020, sont désormais acceptées par des fabricants comme Dell, Lenovo et HPE pour leurs contrats grands comptes, car elles alignent leurs pratiques de sécurité firmware sur les exigences des certifications ISO 27001 et NIS 2 de leurs clients. La pression réglementaire européenne, via le Cyber Resilience Act (CRA) entrant en vigueur en 2027, imposera d'ailleurs à tous les fabricants d'équipements connectés vendus en Europe des obligations légales de mise à jour de sécurité pendant la durée de vie du produit — une évolution majeure qui transformera structurellement les pratiques du marché firmware.

Que se passe-t-il si mon firmware est corrompu intentionnellement ?

Si CHIPSEC ou un outil d'attestation TPM détecte une anomalie firmware (hash PCR divergent, modification de la SPI flash), la procédure à suivre dépend de la nature de l'équipement et de la sensibilité de l'environnement. Pour un laptop ou un poste de travail, la réponse standard est

l'isolation réseau immédiate suivie d'une réinstallation complète depuis une image certifiée — y compris un reflashing du firmware depuis un support de confiance (clé USB bootable avec l'image officielle signée du fabricant). Pour un serveur de production, le processus est plus complexe : l'isolement doit être coordonné avec les équipes d'exploitation pour minimiser l'impact sur les services, et la procédure de reflashing doit être testée en environnement staging avant d'être appliquée en production. Dans les deux cas, **ne jamais tenter de "réparer" un firmware potentiellement compromis via les outils de mise à jour standard** — si le bootkit a patché les routines de mise à jour elles-mêmes (comme le fait CosmicStrand), la mise à jour du firmware via les canaux normaux ne supprimera pas le bootkit et pourrait même consolider sa persistance.

Windows Defender System Guard : l'attestation dynamique en pratique

Windows Defender System Guard Secure Launch (aussi connu sous l'acronyme DRTM, Dynamic Root of Trust for Measurement) est une fonctionnalité introduite dans Windows 10 version 1809 qui exploite les capacités Intel TXT ou AMD SKINIT pour établir un point de mesure de confiance indépendant du firmware UEFI. Contrairement à la chaîne de mesure statique (SRTM) qui commence à la mise sous tension et peut être compromise si le firmware est corrompu, DRTM utilise une instruction processeur spéciale pour réinitialiser les PCR TPM à un état connu et mesurer uniquement le code de lancement Secure Launch Policy Module — un composant Microsoft signé, de petite taille et dont la surface d'attaque est minimale. **Cette approche signifie que même si le firmware UEFI est totalement compromis par un bootkit comme BlackLotus, le DRTM peut détecter l'anomalie car les mesures PCR 17-22 (réservées à DRTM) divergeront des valeurs attendues**, déclenchant une alerte via Windows Health Attestation Service transmise au SIEM.

Pour les équipes de sécurité françaises déployant des postes Windows 11 avec la génération de processeurs Intel 12e ou AMD Zen 4, l'activation du Secure Launch (via GPO : Computer Configuration → Administrative Templates → System → Device Guard → Turn on Virtualization Based Security, avec Secure Launch Configuration = Enabled) est une mesure de durcissement à fort rapport coût/bénéfice. Elle est incluse dans le benchmark CIS Windows 11

Level 2 et constitue l'une des recommandations de sécurité avancées de l'ANSSI pour les postes de travail des administrations françaises. La combinaison DRTM + HVCI + Credential Guard dans un déploiement Secured-Core PC offre une résilience anti-bootkit inégalée par toute autre solution logicielle, rendant l'exploitation d'un bootkit UEFI quasiment impossible sans compromettre physiquement le matériel ou exploiter une vulnérabilité dans le firmware du processeur lui-même — une barre très haute que seuls les acteurs étatiques les plus sophistiqués peuvent franchir.

Les organisations françaises soumises à NIS 2 ou appartenant à un secteur régulé par l'ANSSI doivent documenter leur politique de gestion firmware dans leur SMSI, avec des procédures d'audit CHIPSEC et de vérification d'attestation TPM incluses dans le plan de contrôle annuel.

Conclusion

Ce sujet s'inscrit dans un contexte de menaces en constante évolution. La meilleure protection combine veille active, audits réguliers et sécurité by design. Pour approfondir ou évaluer votre exposition, consultez nos experts.

Vous souhaitez en savoir plus ou évaluer votre exposition ?

Contacter nos experts ou contactez-nous directement.