

Windows Internals : Structures Noyau

3 mai
2026Mis à jour le 17 mai
202648 min de
lecture9614
mots

Comprendre les mécanismes internes du noyau Windows est une compétence fondamentale pour la recherche en vulnérabilités, le développement d'exploits, l'analyse de malwares avancés ou la sécurité endpoint. Le noyau Windows NT, dont l'architecture remonte à la version 3.1 de 1993 mais qui a considérablement évolué avec Windows 11 24H2 et Windows Server 2025, présente une organisation complexe et hautement interconnectée. Les structures comme *EPROCESS* et *ETHREAD* représentent les objets de base, tandis que les attributs de sécurité, le *PEB* (Process Environment Block) et le *TEB* (Thread Environment Block) sont directement accessibles en mode utilisateur. La manipulation de ces structures est au cœur de techniques avancées comme l'injection APC, le vol de token de sécurité, le hooking SSDT, et l'exploitation du processus interne de Windows depuis les structures de base jusqu'aux mécanismes de protection du noyau, passant par les techniques d'exploitation historiques et contemporaines qui ont façonné la sécurité de ce système d'exploitation.

Comprendre les mécanismes internes du noyau Windows est une compétence fondamentale pour la recherche en vulnérabilités, le développement d'exploits, l'analyse de malwares avancés ou la sécurité endpoint. Le noyau Windows NT, dont l'architecture remonte à la version 3.1 de 1993 mais qui a considérablement évolué avec Windows 11 24H2 et Windows Server 2025, présente une organisation complexe et hautement interconnectée. Les structures comme *EPROCESS* et *ETHREAD* représentent les objets de base, tandis que les attributs de sécurité, le *PEB* (Process Environment Block) et le *TEB* (Thread Environment Block) sont directement accessibles en mode utilisateur. La manipulation de ces structures est au cœur de techniques avancées comme l'injection APC, le vol de token de sécurité, le hooking SSDT, et l'exploitation du processus interne de Windows depuis les structures de base jusqu'aux mécanismes de protection du noyau, passant par les techniques d'exploitation historiques et contemporaines qui ont façonné la sécurité de ce système d'exploitation.

Réponse sous 24h

Devis
gratuit

À RETENIR

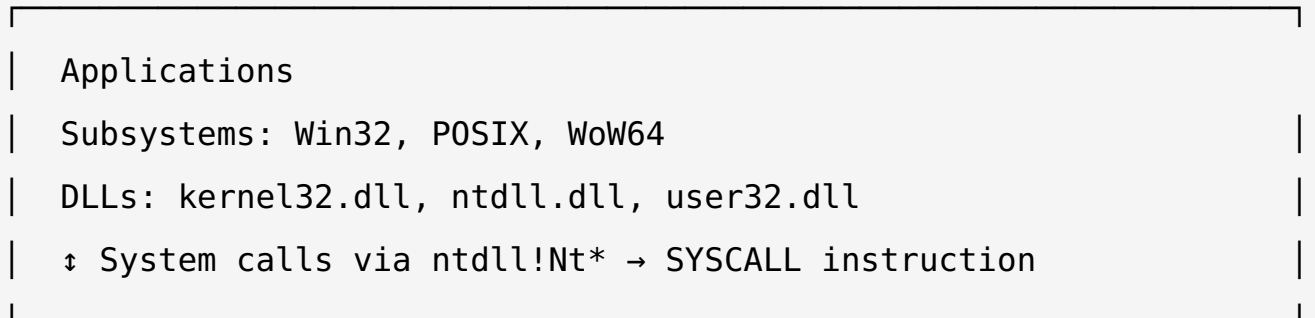
Points clés : Les structures noyau Windows évoluent à chaque version majeure dynamiquement via WinDbg ou les PDB publics de Microsoft. PatchGuard (K PatchGuard) Windows 10 20H1 rendent le patching direct du noyau extrêmement difficile. L'abus vers l'abus d'interfaces légitimes plutôt que la modification directe de structures.

1. Architecture du noyau Windows : vue d'ensemble

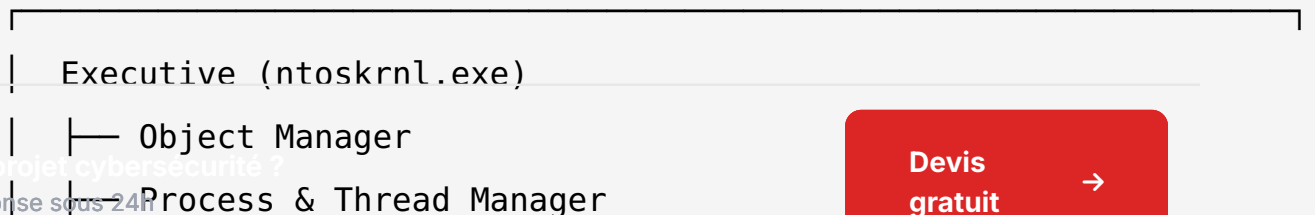
Le noyau Windows s'organise en deux modes d'exécution principaux : le **mode utilisateur** et le **mode noyau**. La frontière entre ces deux modes est appliquée par le processeur via les niveaux de privilèges. Le noyau opère le Executive Windows (Ntoskrnl.exe), les drivers, le HAL (Hardware Abstraction Layer).

Architecture simplifiée Windows NT :

Ring 3 (User Mode)



Ring 0 (Kernel Mode)



En projet cybersécurité ?
Réponse sous 24h

Devis
gratuit →

Réponse sous 24h

Devis
gratuit →