AYI NEDJIMI Consultants

Windows Internals : Structures No

3 mai 2026 • Mis à jour le 17 mai 2026 • 48 min de lecture • 9614 mots •

> Comprendre les mécanismes internes du noyau Windows est une compét
> recherche en vulnérabilités, le développement d'exploits, l'analyse de mal
> sécurité endpoint. Le noyau Windows NT, dont l'architecture remonte.

Comprendre les mécanismes internes du noyau Windows est une compétence fo
vulnérabilités, le développement d'exploits, l'analyse de malwares avancés ou la c
Windows NT, dont l'architecture remonte à la version 3.1 de 1993 mais qui a consi
Windows 11 24H2 et Windows Server 2025, présente une organisation complexe e
interconnectées. Les structures comme *EPROCESS* et *ETHREAD* représentent les
attributs de sécurité, tandis que le *PEB* (Process Environment Block) et le *TEB* (Th
accessibles en mode utilisateur. La manipulation de ces structures est au cœur de
l'injection APC, le vol de token de sécurité, le hooking SSDT, et l'exploitation du po
interne de Windows depuis les structures de base jusqu'aux mécanismes de prote
passant par les techniques d'exploitation historiques et contemporaines qui ont fa

À RETENIR

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

1. Architecture du noyau Windows : vue d'ensemble

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

```
Architecture simplifiée Windows NT :

Ring 3 (User Mode)
┌──────────────────────────────────────────────────────────────┐
│  Applications                                                │
│  Subsystems: Win32, POSIX, WoW64                             │
│  DLLs: kernel32.dll, ntdll.dll, user32.dll                   │
│  ↕ System calls via ntdll!Nt* → SYSCALL instruction          │
└──────────────────────────────────────────────────────────────┘

Ring 0 (Kernel Mode)
┌──────────────────────────────────────────────────────────────┐
│  Executive (ntoskrnl.exe)                                    │
│  ├── Object Manager                                          │
│  ├── Process & Thread Manager                                │
```

Réponse sous 24h

Devis gratuit →