Détection Manuelle du Débogueur (PEB)

Localisation: `0x004044DF` **Fonction:** `sub\_4044B0`
Type: Anti-debug / Evasion **Sévérité:** High

Code Assembleur

```
; Acces manuel au TEB puis au PEB pour verifier le flag BeingDebugged
mov     ebx, 28h
mov     ecx, 2
mov     eax, fs:[ebx+ecx*4]    ; EAX = Adresse du PEB (FS:[30h])
mov     edx, eax
cmp     byte ptr [edx+2], 0    ; Verifie l'offset +2 (BeingDebugged)
jnz     loc_4045F0             ; Saute vers la sortie d'echec si
    detecte
```

Code Décompilé (Reconstitution)

```
// Verification combinee API et acces direct memoire
CheckRemoteDebuggerPresent(GetCurrentProcess(), &pbDebuggerPresent);

// Lecture directe du segment FS
PEB* peb = (PEB*)__readfsdword(0x30);
if (peb->BeingDebugged == 1) {
    return 0; // Echec silencieux
}
```

Analyse

Le binaire utilise une technique d'anti-débogage classique mais obfusquée par des calculs d'index sur le segment FS. Il récupère l'adresse du **Process Environment Block (PEB)** à l'adresse `FS:[0x30]` et vérifie le champ `BeingDebugged` (offset 0x02). Si ce champ est à 1 (présence d'un débogueur), le programme branche vers `loc_4045F0`, qui nettoie la pile et retourne 0, empêchant l'exécution de la logique de décodage.