Opaque Predicate (Saut Impossible)

Localisation: `0x00404540` **Fonction:** `sub_4044B0`
Type: Obfuscation **Sévérité:** Medium

Code Assembleur

```
        ; Calcul préalable: 0x2A (42) * 0x11 (17) = 0x2CA (714)
mov     eax, [esp+6Ch+var_30] ; Charge 714
test    eax, eax              ; Teste les flags sur un nombre positif
js      loc_4046D8            ; "Jump if Sign" (ne saute jamais car
    positif)
```

Analyse

Une structure de contrôle trompeuse (Opaque Predicate) est utilisée pour masquer le chemin vers la routine de succès. Le programme effectue une multiplication dont le résultat (714) est toujours positif. L'instruction `js` (Jump if Sign) teste si le résultat est négatif. Dans un flux normal, ce saut n'est jamais pris, cachant ainsi le bloc de code situé en `loc_4046D8` aux outils d'analyse statique. Ce bloc caché contient l'appel à `puts` permettant d'afficher la chaîne secrète.