

# Skrývání DLL knihoven v běžícím procesu s využitím struktury PEB

Vložil/a [RubberDuck](#) [1], 29 Srpen, 2011 - 14:54

- [Programming](#) [2]
- [Virus & Worms](#) [3]

Autoři malware mají snahu ukrývat své výtvořky nejen před zraky uživatelů, ale taktéž i před 'zraky' různých analyzátorů a detektorů. Důvod je zřejmý: Udržet svůj kód co nejdéle neviditelný znamená jeho vyšší životnost. K tomuto účelu autoři nejen oprašují a renovují již dříve známé techniky, ale vyvíjejí i nové. Jednou ze starších technik je skrývání modulů v běžícím procesu s využitím struktury PEB.

<http://bflow.security-portal.cz/skryvani-dll-knihoven-v-bezicim-procesu-s-vyuzitim-struktury-peb/> [4]

### URL článku:

<https://security-portal.cz/blog/skr%C3%BDv%C3%A1n%C3%AD-dll-knihoven-v-b%C4%9B%C5%BE%C3%ADc%C3%ADm-procesu-s-vyu%C5%BEit%C3%ADm-struktury-peb>

### Odkazy:

[1] <https://security-portal.cz/users/rubberduck>

[2] <https://security-portal.cz/category/tagy/programming>

[3] <https://security-portal.cz/category/tagy/virus-worms>

[4] <http://bflow.security-portal.cz/skryvani-dll-knihoven-v-bezicim-procesu-s-vyuzitim-struktury-peb/>