



Počítačové viry a bezpečnost počítačových systémů

Protokol z předmětu (4b)



Tématická oblast: DLL injection

Přednášející: prof. Ing. Ivan Zelinka, Ph.D.; Ing. Jan Plucar

Jméno a číslo studenta: Daniel Trnka, TRN0038

Datum vypracování: 6. 4. 2019

Zadání:

- 1) Seznamte se s technikou DLL injection a užívanými technikami.
- 2) Vyberte si jednu z metod DLL injection (krom Appinit_DLLs registry) a naprogramujte aplikaci umožňující DLL injection dle Vámi vybrané metody.

BODOVÁNÍ:

Metoda Windows hooks – minimum bodů

Metoda "LoadLibrary" a "WriteProcessMemory" – plný počet bodů

Jiná metoda – dle obtížnosti

- 3) Vytvořte DLL knihovnu, která bude obsahovat libovolnou (smysluplnou) funkci, jež se provede po úspěšném zavedení. Můžete využít kód malware z minulých cvičení.
- 4) Přes Vaši aplikaci proved'te DLL injection vytvořené knihovny do zamýšleného (běžícího) procesu.

Závěr:

Diskutujte následující témata:

- 1) Co je DLL injection? Diskutujte možná využití v praxi.
- 2) Detailněji popište, jak funguje Vámi vybraná metoda DLL injection a dle vybrané metody odpovězte na následující otázky:
 - a) Co se stane po ukončení obslužné (útočnickově) aplikaci, běží-li nadále původní (napadená) aplikace? Bude knihovna stále vykonávat svoji funkci?
 - b) Jak se DLL injection projevívá v task manageru?