Zadanie – Tímový projekt

Ransomvér sa radí medzi najväčšie a najdôležitejšie hrozby súčasnosti. Cieľom tímového projektu je pripraviť komplexnú analýzu vzoriek súčasného malvéru. Očakáva sa výskum šifrovacích schém (manažment kľúčov, šifrovací algoritmus a pod.), obfuskácie, techník na ukrývanie sa do cudzích procesov, ochrany voči ladeniu alebo techník na eskaláciu privilégií. Riešitelia sa počas projektu naučia pracovať so širokou škálou nástrojov vrátane systémových tracerov, dekompilátorov a analyzátorov binárnych súborov. Výstupom práce môžu byť pomocné skripty pre analýzu malvéru a spísanie štandardných procedúr používaných pri analýze. Výstupy projektu plánujeme vydať v odbornom časopise. Očakávaný plán projektu:

1. Nájdite a stiahnite vzorky moderného ransomvéru (nie starší ako rok)
2. Vykonajte analýzu podľa pokynov vedúcich projektu
3. Analýzu priebežne dokumentujte
4. Výsledky analýzy spolu s nástrojmi zverejnite na otvorenom repozitári