BIT - Zámer Projektu

| *Meno: Lukáš Štrbo* | *AIS ID: 110903* | *Dátum: 1. 10. 2023* |

Analýza malvéru pod systémom Windows

V projekte sa budeme zameriavať na analýzu odchyteného malvéru pod systémom Windows, ktorý jeho istými časťami pripomína **File Less** malvér, ktorý nie je jednoducho odhaliteľný či detekovateľný.
V projekte si zanalyzujeme dva pohľady - **Red Team** a **Blue Team**.

Red Team - z uhľa pohľadu útočníka, zanalyzujeme akým spôsobom sa takýto malvér chráni pred detekciou, kde a akým spôsobom infiltruje systém a akým spôsobom si udržuje persistenciu a aktualizácie v systéme. `(*)` V konečnom dôsledku si takýto malvér naimplementujeme a pokúsime sa využiť existujúcu zraniteľnosť softvéru, ktorá dovoľuje Remote Code Execution (RCE) čim ukážeme akým spôsobom môžeme napadnúť konečný systém. Daný malvér sa bude približovať **File Less** malvéru avšak s istou persistenciou.
*Malvér bude implementovaný za pomoci **Windows PowerShell**.*

Blue Team - zanalyzujeme si akým spôsobom je možné takýto vírus detegovať, zistiť čo daný malvér môže robiť a akým spôsobom ho odstrániť - tzv. prepojenie Red Team a Blue team a na čo nezabúdať pri odstraňovaní.

`(*)` Poznámka: V prípade identifikovania zdroja, z ktorého malvér pochádza budeme skôr rozoberať Blue Team pohľad ako samotnú implementáciu malvéru (Red Team pohľad)
