Zápisnica k 12. stretnutiu

Stretnutie sa konalo 15.3.2022 na Discorde.

Na stretnutí sa zúčastnili:

Účastník	Rola
Roderik Ploszek	Vedúci tímového projektu
Peter Švec	Vedúci tímového projektu
Pavol Sobota	Vedúci tímu za študentov
Samuel Hudák	Člen tímu
Andrej Tóth	Člen tímu
Martin Bilka	Člen tímu
Michal Grznár	Člen tímu
Adam Štang	Člen tímu

Zápisnicu vypracoval Adam Štang

Vyhodnotenie úloh z predchádzajúceho stretnutia:

1. Pavol Sobota pracuje na vzorke Virlock ransomvéru a začal ho analzyovať.
2. Andrej Tóth pozeral alternatívy sandboxov na analýzu ransomvérov a našiel niektoré zaujímavé: JoeSandbox, fame, cuckoo 3.
3. Samuel Hudák si vybral vzorku AvosLocker a začal ju reverzovať.
4. Michal Grznár začal analyzovať vzorku WannaCry a študovať si o nej.
5. Martin Kudlačík nebol prítomný ale vieme že začal reverzovať vzorku Phobos.
6. Martin Bilka našiel zaujímavý nástroj na analýzu vzoriek ktorý je online – unpack.me

Opis stretnutia:

1. Viedli sme debatu ohľadne vzoriek ktoré analzyovali v minulosti naši vedúci tímového projektu pretože nie všetky sú úplne dokončené a mohli by sme v nich pokračovať a to konkrétne – samsam – c#, clop – c++, ryuk – c++, lilocker – linux, Katyusha – OpenSSL, ak by sme chceli pokračovať v analýze niektorého zo spomenutých ransomvérov treba napísať vedúcim tímového projektu ktorý nám poskytnú poznámky z analýzy od ktorých sa môžme odpichnúť.

Rozdelenie úloh na nasledujúce dva týždne:

1. Pokračovať v analýze vzoriek.
2. Andrej Tóth skúsi rozbehať cuckoo 3.