Предлог пројекта – Марко Петровић

Моја идеја је да направим модел који ће коришћењем машинског учења препознавати извршне фајлове као безопасне или као малвер.

Старији приступ који су антивируси користили је да поседују ручно направљену базу малвера у којој су малвери описани неким својим карактеристикама, а антивируси су само проверавали да ли се фајл који скенирају налази у бази. Овакав начин рада захтева стално ажурирање базе података и није могуће детектовати малициозне фајлове све док се не појаве у бази. Карактеристике које се користиле за описивање малвера у бази формирају јединствену сигнатуру (fingerprint) вируса која је осетљива на веома мале промене у извршном фајлу, а за сваку промену се мора правити ново правило детекције.

Антивируси који користе машинско учење су много флексибилнији па могу да сами закључе да су слични фајлови малициозни без тога да су сваки од њих видели на тренингу, а могу и да донесу закључке о потпуно новим фајловима те се много лакше прилагођавају растућем броју малвера.

Референца: https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf