LabOs Exercises 4

Hessam Koucheki | 9812358032

Bu-Ali Sina University

Spring 1401

مقدمه:

در این برنامه ما باید با استفاده از زبان برنامه نویسی پایتون، اطلاعات سیستمی مانند میزان مصرف حافظه، میزان مصرف سی‌پی‌یوی لحظه‌ای، میزان مصرف شبکه یا همان سرعت دانلود یا آپلود، و موارد اینچنینی را از سیستم دریافت و پردازش میکردیم.

چگونه میتوان از این اطلاعات برای شناسایی بدافزار استفاده کرد؟

طرز کاری که اکثر آنتی‌ویروس‌ها دارند، استفاده از همین داده‌ها و تحلیل آن‌ها در گذر زمان است. به این صورت که برنامه‌های سیستم‌عامل، مشخص است که چه کاری انجام میدهند و داده‌های عجیب و غریب و یا خارج از قاعده ارسال یا دریافت نمیکنند. ولی برنامه‌های مخرب، مثل ویروس‌ها یا کرم‌ها، منابع سیستم را به طور مشکوک و غیر نرمالی مصرف میکنند. از همین رو یکی از راه‌های شناسایی آن‌ها استفاده از تغییر بار و میانگین سیستم است، به این صورت که مثلا اگر در ده دقیقه گذشته مصرف اینترنت، ده مگابایت به ازای هر دقیقه بوده است، و ناگهان تبدیل به 30 مگابایت در دقیقه میشود، و میدانیم که هیچ برنامه تایید شده‌ای در حال اجرا و ارسال و دریافت اطلاعات نیست، پس میتوانیم این نتیجه گیری را کنیم که احتمالا برنامه‌ای مخرب در پس زمینه در حال اجرا است و احتمالا دارد دیتای مارا میدزدد و آنتی ویروس ها از این روش برای شناسایی پراسس های مخرب استفاده میکنند و از ادامه فعالیت آن‌ها جلوگیری میکنند.